

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



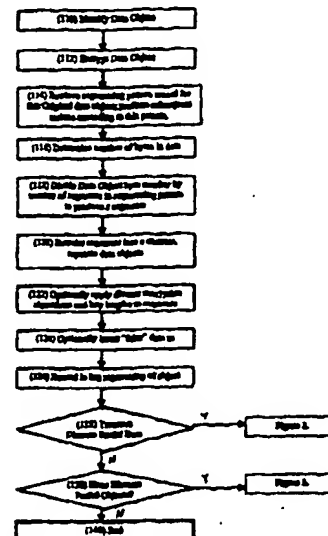
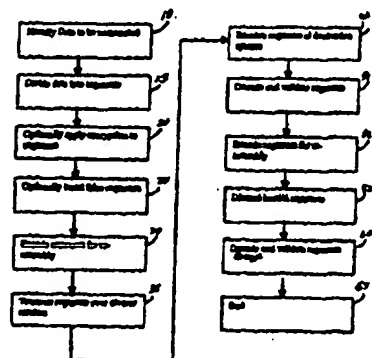
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04L 12/56, H04J 3/24		A1	(11) International Publication Number: WO 00/04681
			(43) International Publication Date: 27 January 2000 (27.01.00)
(21) International Application Number: PCT/US99/16087			(81) Designated States: AE, JP, US, ZA, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
(22) International Filing Date: 16 July 1999 (16.07.99)			
(30) Priority Data: 60/093,106 16 July 1998 (16.07.98) US			
(63) Related by Continuation (CON) or Continuation-in-Part (CIP) to Earlier Application US 60/093,106 (CIP) Filed on 16 July 1998 (16.07.98)			
(71)(72) Applicant and Inventor: LAMBERT, Francis [US/US]; 1901 Spruce Street, Boulder, CO 80302 (US).			
(74) Agents: PANG, Stephen, Y. et al.; Townsend and Townsend and Crew LLP, 8th floor, Two Embarcadero Center, San Francisco, CA 94111 (US).			

Published
With international search report.

(54) Title: METHOD FOR SECURE DATA TRANSMISSION AND STORAGE

System Flowchart



(57) Abstract

A method for transmitting data from a first computer to a second computer includes identifying data to be transmitted (10), segmenting the data (15) into a plurality of data packets, the plurality of data packets including at least a first plurality of data packets and a second plurality of data packets, specifying a first transmission (35) carrying medium for transmission of the first plurality of data packets, specifying a second transmission carrying medium for transmission of the second plurality of data packets, transmitting the first plurality of data packets to the first computer network backbone, and transmitting the second plurality of data packets to the second computer network backbone.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

METHOD FOR SECURE DATA TRANSMISSION AND STORAGE

5 CROSS-REFERENCES TO RELATED APPLICATIONS

This application claims the benefit and priority of U. S. Provisional Patent Application No. 60/093,106, filed July 16, 1998, entitled Method for Secure Data Transmission (Attorney Docket No. 18930-000400). This application is hereby incorporated by reference for all purposes.

10

BACKGROUND OF THE INVENTION

This invention relates to methods for using and storing secure data. More specifically, the invention relates to a data processing, transmission, and storage methods where an original data object is segmented, and reordered into discrete and separate
15 encrypted data objects, none of which contain a complete representation of the original data object, and whereby these discrete data objects are transmitted via separate data carriers, or different network infrastructure elements, or via different transmission media, or at different times, or are stored in different locations so as to limit acquisition and decryption of the original data object.

20 The advent of digital data transmission and storage has prompted more and more organizations and individuals to employ digital systems to convey, receive and retain digital information. Digital information may include, for example, business records, electronic documents, pictures, video data, audio data, real time measurements, electronic commerce transactions, personal and work-related e-mail, advertisements, and the like.

25 For sensitive digital data, security is becoming an important consideration when being transmitted across public computer networks. Types of sensitive digital data may include personal data, financial data, health data, data that sensitive in nature, data which a user wants to prevent from being exposed, and the like. Because unauthorized individuals, "hackers" or "crackers," are constantly developing new methods and systems for eavesdrop,

“sniff”, “hack”, or otherwise gain access to sensitive digital data, higher security of such digital data is needed.

Many innovations have emerged to protect the privacy and security of digital information. For example, some conventional forms of security systems include firewalls, data encryption, data encoding, digital signatures, hashing, passwords, biometric identification, and the like. These systems and methods generally include capabilities to either restrict access to data or transform the data into values which are difficult to transform back into the original data values. Thus, the data transmitted or stored by these innovations can be protected from facile discovery by unauthorized access. Unfortunately, innovation have also occurred on the part of hackers, thus systems and methods for secure transmission of data must also evolve.

The level of security of the transmitted data is often dependent upon the ability of the hacker to decrypt the data, thus, it is often desirable to prevent hackers and other unauthorized entities from accessing, acquiring, or decrypting the data. Most current data security systems are eventually defeated by inventive, persistent, yet unauthorized hackers by brute force. Further, hacking techniques are often widely published on the Internet. As a result, digital data is often most vulnerable while being transmitted across public networks.

Thus what is needed are security methods that overcomes the foregoing drawbacks and renders more difficult the unauthorized access to digital data.

20

SUMMARY OF THE INVENTION

The present invention provides processes for the manipulation, transmission, and storage of data that allows users of the data to more securely transmit and store the data. The security is provided through a process providing beneficial utilization of the phenomenon of “bit degradation” occurring in many types of data encryption methods, which is the condition that an encrypted data object cannot be decrypted if any of the bits of the encrypted data object are not present.

The Invention provides processes for reordering segments of an original encrypted data object into discrete, separate data objects. These discrete data objects can have false data segments inserted, or “salted”, into them, have the encrypted data object segments reordered, or have certain segments re-encrypted with varying encryption algorithms and/or key lengths. The pattern by which the “disassembly” process of the

Invention divides, reorders, "salts", or re-encrypts the data segments of the complete original encrypted data object are able to be reversed by the "re-assembly" process of the Invention in such as a manner as to restore the original encrypted data object from the various discrete partial, reordered data objects.

5 These discrete partial data objects can be transmitted over different data carriers, over different network infrastructure elements such as Internet Backbones, different packet routing routes, different transmission media, or at different times, or in any combination thereof, so as to render more difficult the acquisition of the complete original encrypted data object during transmission. The receiving system can accumulate, disassemble,
10 and reorder the transmitted packets so as to reconstruct the original encrypted data object. If any discrete partial data objects do not arrive at the receiving system, it can request to the sending system that it resend that object.

 Further, these discrete data objects, whether or not they are transmitted, can be stored in different locations, on different storage media, or in different storage system access
15 areas, or any combination thereof, so as to render more difficult the access to the complete original encrypted data object during storage.

 If the original encrypted data object was encrypted by an encryption methodology that renders the encrypted data unable to be decrypted in the case of "bit degradation" or other phenomena resulting from the absence of encrypted data, then using the
20 Invention to limit the ability of unauthorized accessors to acquire, access, and/or re-assemble the entire original encrypted data object will prevent them from being able to decrypt the original encrypted data object or any portion thereof.

 Further, the Invention can provide that a data transmission utilizing symmetric key encryption pass the symmetric session key with greater security when different and
25 discrete partial segments of the complete key are transmitted in reordered segments, over different data carriers using different transmission infrastructure or enforcing data packet routing over different routers, over different types of transmission media such as IP networks, wireless networks, analog switching networks and the like, or any combination thereof, or at different times.

30 Further, the Invention can provide an increase in the security of a stored contiguous object of encrypted data when different and discrete partial segments of the complete decryption key for that data object are stored in reordered segments, in different

locations, on different storage media, in different storage system access areas, or any combination thereof.

The Invention is easily and effectively executed using small encryption keys on low-cost computing equipment. It provides strong security even with small encryption
5 keys since the absence of even one bit of the original encrypted data object will render the remaining encrypted data bits into undecryptable ciphertext, and therefore unusable by the unauthorized accessors of discrete partial data segments.

In one embodiment, an object of unencrypted data is provided. Also provided is an encryption method that renders the encrypted data undecryptable if any of the resulting
10 encrypted data bits are absent. Also provided is a process for segmenting, or "disassembling", an encrypted data object into discrete segments. Also provided is a process for assembling the discrete segments into separate segment groupings, each containing a portion of the original encrypted data object. Further provided is a method for transmitting these separate segment groupings over different data routings. Also provided is a process for receiving
15 these separate segment groupings from different data routings. Also provided is a process for segmenting the received segment groupings back into the original discrete segments of the original encrypted data object so as to allow the "re-assembly" of the discrete segments into the original encrypted data object. Also provided is a method for decrypting the original data object into the originating object of unencrypted data.

20 In another aspect of the invention a segmenting method is provided that reorders the segments of the segmented original encrypted data object or a segmented encryption key into a contiguous, reordered data object according to a pattern that is structured so as to be reversed by the "re-assembly" process that reconstructs the original encrypted data object or encryption key.

25 In another aspect of the invention a segmenting method is provided that inserts segments of "false" or unrelated data to the original encrypted object or segmented encryption key according to a pattern that is structured so as to allow the "re-assembly" method to discard the unrelated data during the process of re-assembling the original encrypted data object or encryption key.

30 In another aspect of the invention a segmenting method is provided that re-encrypts various segments of the original encrypted data object or segmented encryption key using various encryption key lengths and algorithms according to a pattern that is structured

so as to allow the "re-assembly" method to discard the decrypt the re-encrypted data segments during the process of re-assembling the original encrypted data object or encryption key.

In another aspect of the invention a transmission method is provided that
5 transmits discrete data objects of original encrypted data segments or segmented encryption key via different combinations of transmission media, such as the Internet, cellular phones, wireless data carriers, analog telephone switches, packet switched radio, and others. Also provided is a data receiving method that receives the discrete data objects from the various transmission media upon which they were transmitted so as to allow the "re-assembly"
10 method to re-assemble the original encrypted data object or encryption key.

In another aspect of the invention a transmission method is provided that transmits discrete data objects of original encrypted data or encryption key segments via transmission protocols that enforce a pre-determined or differentiated packet routing from the routing of other associated discrete data objects derived from the same original encrypted
15 data segment. This could include sending discrete data objects using static IP delivery rules programmed into a packet routing device. Also provided is a data receiving method that receives the discrete data objects from the differentiated packet routing so as to allow the "re-assembly" method to re-assemble the original encrypted data object or encryption key.

In another aspect of the invention a transmission method is provided that
20 transmits discrete partial data objects of original encrypted data or encryption key segments by using individually or in combination diverse transmission protocols, such as FTP, SMTP, HTTP, and the like, as well as such proprietary transmission protocols as can be devised. Also provided is a data receiving method that allows the corresponding destination systems to receive the discrete data objects by using individually or in combination diverse transmission
25 protocols, such as FTP, SMTP, HTTP, and the like, as well as such proprietary transmission protocols as can be devised, so as to allow the "re-assembly" method to authenticate, and process them in order to re-assemble the original encrypted data object or encryption key.

In another aspect of the invention a transmission method is provided that transmits discrete partial data objects of original encrypted data or encryption key segments
30 to diverse destination systems or to diverse transmission protocol addresses. Also provided is a data receiving method that allows the corresponding diverse destination systems or diverse

transmission addresses to receive the discrete data objects so as to allow the "re-assembly" method to re-assemble the original encrypted data object or encryption key.

5 In another aspect of the invention a transmission method is provided that transmits discrete data objects of original encrypted data segments or a segmented encryption key from various transmission systems or various transmission protocol addresses. Also provided is a data receiving method that allows the corresponding destination systems or transmission addresses to receive the discrete data objects from various transmission systems and various transmission system addresses so as to allow the "re-assembly" method to re-assemble the original encrypted data object or encryption key.

10 In another aspect of the invention a transmission method is provided that transmits discrete data objects of original encrypted data segments or a segmented encryption key during varying time intervals. Also provided is a data receiving method that receives the discrete data objects during various time intervals so as to allow the "re-assembly" method to re-assemble the original encrypted data object or encryption key.

15 In another aspect of the invention a transmission method is provided that transmits an announcement object to the receiving system to alert it to receive discrete data objects of original encrypted data segments or a segmented encryption key. Also provided is a data receiving method that receives the announcement object so as to allow the receiving system to retrieve a reception pattern record and prepare various reception sub-systems for
20 reception and processing of the discrete partial data objects.

In another aspect of the invention a data reception method is provided that times out the reception of discrete data objects of original encrypted data segments or a segmented encryption key according to the delivery latency tolerance parameters contained in the data object reception pattern record. Also provided is a data reception method that
25 transmits a request to the originating transmission system or systems, requesting a re-transmission of any data objects that do not arrive within the delivery latency tolerance parameters. Also provided is a data transmission method that allows an originating transmission system to receive, authenticate, process, and re-transmit a data object that was requested by the reception system for re-transmission.

30 In yet another embodiment, a storage method is provided that stores discrete, separate data groupings of a segmented original data object or encryption key in diverse data storage locations. Also provided is a data retrieval method that retrieves the discrete, separate

groupings of the original encryption key from diverse storage locations so as to allow the "re-assembly" method to re-assemble the original encrypted data object or encryption key.

In another aspect of the invention a storage method is provided that stores discrete, separate data groupings of a segmented original data object or a segmented encryption key in diverse system access areas so as to require diverse authentication events to allow storage, acquisition and re-assembly of the segments contained in the discrete, separate data groupings. Also provided is a data retrieval method that performs required authentication events to retrieve the discrete, separate data segment groupings from diverse storage locations so as to allow the "re-assembly" method to re-assemble the original encrypted data object or encryption key.

In another aspect of the invention a storage method is provided that stores discrete, separate data groupings of a segmented original data object or a segmented encryption key separately on diverse storage media and devices so as not to allow exposure of a complete representation of the original encrypted data or a segmented encryption key to theft, destruction, or failure of a storage medium or device. Also provided is a data retrieval method that retrieves the discrete, separate groupings from diverse storage locations so as to allow the "re-assembly" method to re-assemble the original encrypted data object or encryption key.

Further, these discrete data objects can be stored in different locations, on different storage media, or in different storage system access areas, or any combination thereof, so as to render more difficult the access to the complete original encrypted data object during storage.

Additional aspects and embodiments of the present invention will become apparent upon a perusal of the following detailed description and accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1a is an overview flow diagram of an embodiment of the present invention;

Fig. 1b is a procedural flow diagram for the disassembly of Original Data Objects into Discrete Partial Data Segment Objects according to an embodiment of the present invention;

Fig. 2 is a procedural flow diagram for the preparation for transmission of Discrete Partial Data Segment Objects according to an embodiment of the present invention;

Fig. 3 is a procedural flow diagram for the transmission of Discrete Partial Data Segment Objects according to an embodiment of the present invention;

5 Fig. 4 is a procedural flow diagram for the reception of Discrete Partial Data Segment Objects according to an embodiment of the present invention;

Fig. 5 is a procedural flow diagram for the storage of Discrete Partial Data Segment Objects according to an embodiment of the present invention;

10 Fig. 6 is a procedural flow diagram for the retrieval from storage of Discrete Partial Data Segment Objects according to an embodiment of the present invention;

Fig. 7 and 8 are procedural flow diagrams for the re-assembly of Discrete Partial Data Segment Objects into Original Data Objects according to an embodiment of the present invention;

15 Fig. 9 is a diagram illustrating a transmission network using an embodiment of the present invention;

Fig. 10 is a diagram illustrating a storage network using an embodiment of the present invention; and

Figs 11-14 illustrates enhancements to embodiments of the present invention.

20 DESCRIPTION OF THE SPECIFIC EMBODIMENTS

Fig. 1a illustrates an flow diagram according to an embodiment of the present invention. In particular, Fig. 1a illustrates an overview of a method for securely transmitting data from a first computer to a second computer.

Initially, the data to be transmitted securely is determined by a sending
25 computer, step 10. The data may include textual data such as documents, spreadsheets, credit card, financial information, form submissions, or the like; images data such as facsimiles, scans, or the like; and other types of data. Typically, the data is then divided into groups of discrete data segments, step 15. For example, the data may be divided into two or more groups of discrete data segments. In one example, one group of discrete data segments
30 includes all even-numbered data segments, and the other group of discrete data segments includes all the odd-numbered data segments. In other embodiment, one group of data

segments includes every fifth data segment, and the other group of data segments includes the remaining data segments.

Next, in one embodiment of the present invention, data segments may be encrypted, step 20. In this embodiment all data segments may be encrypted. In alternative
5 embodiments, a predetermined number or pattern of data segments are encrypted, for example, every odd numbered data segment is encrypted. The type of encryption can vary and any conventional encryption scheme can be used, for example symmetric, asymmetric, and the like.

In the present embodiment, one or more dummy data segments may be
10 intermingled or mixed into the groups of data segments, step 25. For example, a random number may be used to form a dummy data segment, and dummy data segments are inserted into the group of data segments after every fourth data segment. The positioning of the dummy data segments within the group of data segments may be maintained for subsequent filtering

15 The dummy data segments and the "valid" data segments are next encoded, step 30. In the present embodiment, the encoding scheme allows the transmitted segments received by a receiving computer to be reassembled into the correct order.

Next, the groups of data segments, step combined dummy and valid, are each transmitted across different a carriers, step 35. In one embodiment where two groups of data
20 segments have been determined, step e.g. odd and even,, a first group of data segments may be transmitted across a computer network; and the second group of data segments may be transmitted across a wireless network. In another embodiment, the first group of data segments may be transmitted across a particular paths, for example, utilizing a first computer network backbone, and the second group of data segments may be transmitted across a
25 different transmission paths, for example, utilizing a second computer network backbone. As will be described further below, may different types diverse communications carriers can be used.

After the data have been transmitted over different carriers, a receiving computer receives the groups of data segments, step 40. In one embodiment of the present
30 invention, the receiving computer has access to both types of communications carriers and then receives the two or more groups of data segments. In another embodiment, a server remote from the receiver has access to both types of communications carriers, receives the

groups of data segments, and receives the two or more groups of data segments. The receiving computer then receives both groups of data segments from the remote server.

In the present embodiment, once the receiving computer receives the groups of data segments, the receiving computer determines whether all, or validates, the groups of data segments have been received, step 45. In one embodiment, the data segments are numbered. In other embodiment, check sums and other techniques may be used to perform an initial validation on the data segments. Next, the encoding scheme used in step 30, above, is used to ensure the data segments are assembled into the correct order, step 50.

The dummy data segments inserted with the valid data segments is then identified and discarded, step 55. In one embodiment, the locations of the dummy data segments may be part of the data transmitted from the sending computer. In another embodiment, the receiving computer knows ahead of time, or through other means which data segments include valid data and which ones include dummy data. The valid data segments are then revalidated and decrypted, as necessary, step 60, in order to recover the data to be transmitted securely.

In the embodiment above, the steps may be re-arranged, and a greater or lesser number of similar steps may be performed in other embodiments of the present invention. A more detailed description of another embodiment is described below.

Figs. 1b through 8 illustrate more detailed flow diagrams according to an embodiment of the present invention. As used herein the term "secure" refers to a transmission or storage of data that limiting the ability of unauthorized entities to access the data object.

Initially, a data object, typically comprising of a binary bit stream is identified, step 110. As disclosed above, the data represented by the bits may include textual data such as documents, spreadsheets, credit card, financial information, form submissions, or the like; images data such as facsimiles, scans, or the like; and other types of data for which secure transmission is desired. The data may be identified by a user, or in another embodiment, the data may automatically be determined by another computer program. An example of the latter case is where all transmissions from a first computer across a network to another computer is to be secured according to the techniques described herein.

The data object may encrypted in step 112. Various encryption methods may be used and are well known. In this embodiment the data object is encrypted using a private

key of an asymmetric dual key system, as is commonly known to those skilled in the art of encrypting data. Alternatively, encryption methods may be used in an embodiment of the present invention that do not use the method described above, but provide an equivalent encryption capability. Further embodiments of the present invention may use encryption techniques where if any bit with the encrypted data object are lost, the entire data object cannot be recovered.

Next, in the present embodiment, a segmenting pattern is determined, step 114. In one embodiment, the segmenting pattern may be generated on the fly, or may be a pre-determined segmenting pattern from a library of segmenting patterns. The segmenting pattern is used to determine how many adjacent data objects will form a segment of data.

The length of the data object is determined for segmenting purposes, and a divisor associated with the segmenting pattern database record are then determined, step 116. The data object is then divided by the divisor into to form segments of data objects from the data objects, step 118. In this embodiment, this technique is used to reduce the amount of computation required for formation of the groups of segments of data objects (data segments), as will be described below. In an alternative embodiment, segments are not needed, and data objects are used to form groups of data objects, as will be described below.

The segments of data objects (data segments) are then reordered and are used to form groups of data segments, step 120. The number of groups are typically predefined. In one embodiment of the present invention, adjacent segments of data objects are placed within different groups. For example, segment 1 is placed in group 1, segment 2 is placed in group 2, segment 3 is placed in group 1, and the like. In another example embodiment, one-half of the segments are placed in group 1 and the other half of the segments are placed in group 2. Further, the ordering of data within segments need not occur in the same order as they occurred in the Original Data Object. In such embodiments, the ordering of the data objects may be stored within the segmenting pattern discussed in step 114, above.

In one embodiment, certain data segments may be encrypted again for further protection, step 122. Diverse encryption algorithms and diverse key lengths may be used at this stage, i.e. encryption using different levels or types of encryption, different key lengths, and the like. It is expected that such a step makes it more difficult for unauthorized users to recover the original data.

In another embodiment of the present invention, blank, false, or dummy data segments may be introduced into different locations into different data segments, step 124. In such embodiments, the location of such dummy data segments could also be determined by the segmenting pattern. In one embodiment, the dummy data segment may include bits from random data generating algorithms, parts of the Original Data Object, or the like. It is also expected that such a step makes it more difficult for unauthorized parties to recover the original data.

The details of the segmenting of the Original Data Object into discrete, partial data groupings, and the like, may be stored in a log file, or the like, step 126. It is then determined whether the groups of segmented data are to be transmitted to another computer system, step 128, or the groups are to be stored in memory, step 130.

Fig. 2 illustrates a flow diagram of an embodiment of the present invention, when data is to be transmitted to another computer server. The method is designed to transmit partial representation of the original data object in such a way as to limit the ability of unauthorized accessors to acquire the data. At this stage, the groups of data segments are typically stored in fast computer memory (e.g. RAM), step 210.

A transmission pattern is then determined, step 212. In the present embodiment, the transmission pattern is used to determine how the groups of data segments are conditioned and eventually transmitted, as will be illustrated below. Next, different transmission parameters for each group of data segments are determined, step 214. In one embodiment, this allows adjacent groups of data segments to be dispersed and dissociate with other adjacent groups during transmission time. Some parameters which may be adjusted may include the transmission media, the time intervals between transmission of the separate objects, data segments, or groups of data segments, the routing of data packets on a network, the network onto which those groups of data segments will be routed, and the like. In another embodiment, authentication and integrity metadata may also be added to the data to validate the data objects upon receipt. In this embodiment, authentication metadata technique may include a PKI digital signature, encrypted with an SHA-1 message digest, step hash, of the discrete data object.

Next, transmission parameters for each group of data segments are set according to the pattern specified in the transmission pattern record, as illustrated in the following steps.

In one embodiment it is determined whether the groups of data segments will use diverse media types, step 216. In this embodiment, media type include transmission over packet-based digital networks, such as the Internet, Central Office telephone switching circuitry, wireless digital transmission using cellular frequencies, and the like. In an alternative embodiment, other groups of data segments may be stored in a physical format, including digital storage media, such as tapes, floppy disks, and optical discs, as well as printed materials, such as barcodes and keyboard entry sequences. Such an embodiment requires unauthorized accessors of the data to monitor many types of media simultaneously in order to capture all groups of data segments to recover the data. The requirement of monitoring resources is expected to be more than the capability of most unauthorized accessors, thus this technique should limit unauthorized users the ability to recover the original data. If diverse media types has been selected, groups of data segments may include appropriate metadata for later processing, step 218.

In one embodiment it is determined whether the groups of data segments will be transmitted to different addresses, step 220. For example, whether a first-half of a transmission will be sent to a network address and a second-half of the transmission will be sent to a second network address. In this embodiment, the source and destination addresses from and to which the groups of data segments are determined, step 222. By using diversified addressing on digital packets, the method forces unauthorized accessors to know the range of addresses to which these groups of data segments will be transmitted, thereby limiting techniques using addressing information to associate and then acquire data packets.

In this embodiment, source and destination addressing is also used to enhance the ability of the packets of a discrete data object to stay on the same routing paths specific and distinct to a particular network service provider or data carrier. If the source and destination addresses of a data packet are both contained in the address space of the service provider or data carrier, the packets typically stay on that provider's network with higher predictability. This is typically because providers tend to route packets on their own carrier infrastructure to avoid charges resulting from switching packets onto other carriers' infrastructures. By addressing groups of data segments to travel to more than one address, unauthorized accessors are forced to monitor multiple infrastructures simultaneously. This greatly increases the cost and effort involved in capturing a complete set of discrete partial

data objects associated with one original data object, thereby limiting the ability of those accessors to acquire, decrypt, and analyze packets.

In one embodiment it is determined whether the groups of data segments will be transmitted at varying time intervals, step 224. In such an embodiment, the transmission
5 time interval parameters specified by the transmission pattern record is written into the metadata associated with each group of data segments. By transmitting data objects at varying time intervals, unauthorized accessors are forced to monitor transmission infrastructures over longer periods of time to increase their chances of capturing all of the partial objects required to reconstruct an original data object. Since the amount of traffic on
10 some networks, such as the Internet, requires substantial data capturing and storage resources to capture the traffic from even a small interval of time, this greatly increases the cost and effort involved in capturing a complete set of discrete partial data objects. It also improves the possibility that the unauthorized accessor will miss capturing some objects, and thereby render all other associated captured objects undecryptable and useless.

In one embodiment it is determined whether the groups of data segments will be sent via a pre-determined routing, step 228. In such an embodiment, the routing information from the transmission pattern record is written into the metadata associated with the groups of data segments, step 230. By transmitting discrete partial data objects over
15 distinct specified routings, advantages are gained which are similar to transmitting them over distinct service providers and data carriers, as described above. The ability of network service providers to specify routing and priority of packets is consistently improving, and such an embodiment provides the capability to use that resource in sending discrete partial data objects over public and private networks.

In one embodiment it is determined whether a specific information transfer
25 protocol for the groups of data segments, step 234. Types of well known transfer protocols includes FTP, HTTP, SMTP. In one embodiment, the ability of the system to specify proprietary transfer protocols known to the receiving system is also envisioned. In such an embodiment, the protocol specification is written into the metadata of the groups of data objects, step 236. By using diverse protocols to transmit data objects, protocol format
30 information is less useful in allowing unauthorized accessors to capture and analyze data packets. Doing so requires that those accessors monitor and capture multiple protocol transmissions from a data source, thereby increasing the cost and effort in doing so.

In one embodiment, transfer protocols have notice and retrieval capabilities, where the originating system is able to request that the receiving system retrieve some of the discrete data objects from a protocol server. This allows the originating system to confirm that the receiving system received some data and also controls the receiving systems access to
5 access the remaining data. This is due to the fact that if the originating protocol server does not release even one partial data object, the receiving system will be unable to decrypt any other associated data objects that it has already acquired.

In one embodiment it is determined whether the groups of data segments specified by the transmission pattern record are to be transmitted from a different
10 transmission system, step 242. In such an embodiment, the intermediary system transfer information specified by the transmission pattern record is written into the metadata associated with each group of data segments, step 244. In one embodiment, some or all of the data can be transferred via a Virtual Private Network, dedicated data line, or other privacy enhanced transmission medium, to another transmission system which in turn sends the
15 groups of data to the receiving system. By transmitting partial objects from multiple systems, unauthorized accessors are forced to monitor the transmission points of multiple transmission systems in order to capture a complete set of partial data objects. This greatly increases the cost and effort of doing so, thereby limiting their ability to perform that action.

In the present embodiment, if the groups of data segments have been
20 processed, they are stored in memory, step 246. Next, the originating system prepares an "announcement object", step 248, which typically comprises metadata for the subsequent data transmission, that has been encrypted and digitally signed, step 250. The announcement object is subsequently transmitted to the intended destination system. This allows the destination system to report a failure if the incorrect number of groups of data segments
25 arrive, and also to know how to recover the original data. In an alternative embodiment, the meta data may be combined with the transmission of the groups of data segments.

Fig. 3 illustrates a flow diagram according to an embodiment of the present invention. In particular, Fig. 3 illustrates the procedures executed by a transmission server when transmitting the groups of data segments.

30 In the present embodiment of the present invention, transmissions of groups of data segments, as well as the announcement object, may be performed by a logical transmission server. In this embodiment, when the transmission server determines that a

group of data segments are ready to be transmitted, step 312, the transmission server transmits the data, step 314. If the transmission server determines that another group of data segments is ready to be transmitted, step 315, the transmission server. When the group of data segments is found, the group is retrieved, step 318.

5 The transmission server then determines whether a time interval has been specified in step 226, step 320. If so, the transmission server determines the time interval, step 322. More specifically, the transmission server reads the metadata from the group of data segments to determine the transmission parameters.

Next, the transmission server then determines whether the groups of data
10 segments are to be transmitted from another system, step 324. As disclosed above, the groups of data segments are subsequently transferred from the other system to the destination server. If so, then it resets the time delay parameter in the object metadata to zero, since that time has already expired. It then passes the group of data segments to a server, step 328, that subsequently transmits the data securely to another system. In the present embodiment, it is
15 envisioned that the other system will send the groups of data segments in a secure manner as described herein, step 332.

In the present embodiment, the transmission server determines whether the groups of data segments are to be sent via non-packet routing transmission media, step 336. In this example, non-packet routing media may comprise Central Office telephone networks
20 including modems, wireless transmission using a cellular transmission infrastructure, and the like. The groups of data segments earmarked for transmission via non-packet routing media, they are placed in an appropriate memory area, step 338. When, the transmission server discovers the presence of the groups of data segments, they are transmitted, step 340.

In one embodiment, the non-packet routing media server dials out on a
25 connected modem to the receiving system, exchanges authentication protocols, and then uploads the groups of data segments to the receiving system. Transmitting data in this manner forces unauthorized accessors to monitor both Central Office type phone lines, and the like, as well as multiple packet routing and non-packet routing simultaneously, greatly lowering the possibility that they will capture and analyze a complete set of groups of data
30 segments.

Next, in this embodiment, the transmission server determines whether groups of data objects are to be transmitted using a pre-determined transmission routing, step 342. If

so, the transmission server determines the transmission routings from step 230, above, and transmits the groups of data segments to the specific router, step 344. In one embodiment of the present invention, this router may be connected to a first ISP that is coupled to a "backbone" network infrastructure element that is different from the backbone network infrastructure coupled to a second ISP to which other routers in the system are connected. This embodiment enables the transmission server to deliberately transmit groups of data segments over different backbones, by directing the transmission server to transmit to different routers. As a result, unauthorized accessors are forced to monitor data traffic on multiple network backbones simultaneously in order to capture all of the groups of data segments. This would greatly raise the cost of attempting to acquire unauthorized access to data, thereby reducing the likelihood of data theft.

In the present embodiment, the transmission server determines whether groups of data segments are to be sent via a known transfer protocol, step 348. This typically occurs by viewing the metadata associated with the groups of data segments defined in steps 234 and 236. If the group of data segments are to be transmitted via a known protocol, the groups of data segments are placed in an appropriate memory location, step 350. Next, the groups are transmitted, and a notification is sent to the destination or receiving system, step 352. Subsequently, the appropriately protocol servers on the originating and destination systems then manage the transfer of data by that protocol. By using multiple protocols, unauthorized accessors are deterred from using protocol stream capture to acquire a complete set of partial data objects. This embodiment also has the advantage of more predictably in transferring data objects through firewall security systems. For example, ports for common protocols are routinely opened on the firewall to allow e-mail, World Wide Web, File Transfer Protocol traffic, and the like to be shared with the network outside the firewall protected network.

Next, the data segment is transferred via a specified default, defined transfer protocol, step 354. In this embodiment, the sending and receiving systems exchange authentication tokens in the form of digital signatures, and then begin upload and capture of the groups of data segments. When data are sent through the routers with varying source and destination addresses, they may be sent across varying network paths. This embodiment deters unauthorized accessors from acquiring a complete set of discrete partial data objects by using packet address analysis. These accessors would be required to know and monitor a broad range of source and destination addresses to and from which the data objects can be

sent, and then be able to monitor and capture all traffic between that range of network addresses.

After the group of data segments has been sent, the process disclosed above may be repeated for the next group of data segments. In no other groups of data segments are
5 available, the process halts, step 334.

Fig. 4 illustrates a flow diagram of an embodiment of the present invention. In particular, Fig. 4 illustrates the process of a destination or receiving system receiving the groups of data segments transmitted in the above described processes.

In this embodiment, if an announcement object was used to transmit metadata
10 for the groups of data segments, the receiving system receives the announcement object, step 410. The metadata typically includes a digital signature from the transmitting system, and encrypted information describing the meta data, and the like. As described above, metadata associated with the groups of data segments may also be transmitted with the groups of data segments. In response to the receipt, the receiving system decrypts the meta data and
15 determines the delivery pattern record, step 412. As disclosed above in steps 248 and 250, the pattern record specifies how groups of data segments are to be transmitted to the receiving system. The method then refers to the delivery pattern record and prepares the system accordingly to receive the data, step 414. In the present embodiment, the system initiates receiving applications for the various ways in which it could receive a data object
20 according to the delivery pattern record. For example, the receiving system initiates reception servers and hardware for various transmission media, including putting a receiving modem into auto answer or clearing a cellular channel for incoming data transfer calls, and the like.

In the present embodiment, the method then sets time parameters for reception
25 according to the delivery pattern record, step 416. This is done so the receiving system can time-out the delivery of data and report possible error conditions. If various known protocol servers are specified in the pattern record, these servers are also initiated, step 418. As previously discussed, such protocol servers may include FTP servers, SMTP servers, and HTTP servers, and the like.

30 Next, the receiving system enters into a program loop that checks for the presence of data, step 420. Delivery of objects can be terminated either through delivery of a complete data set, through a time-out and subsequent failure of the delivery process for the

current group of data segments, and the like. If no further objects are expected to be delivered, step 422, the reassembly process shown in Fig. 7 begins, to reassemble the original data object.

In the present embodiment each group of data segments is tracked in the delivery pattern record to determine when all of the groups of data segments have arrived. In this example, the receiving system references the delivery pattern record to determine when and by which means remaining groups of data segments are to arrive, step 424. If an expected group of data segments has not been received, step 426, the elapsed time is measured against a latency time expected for delivery of the group, step 428. This latency time may also be specified in the delivery pattern record.

In the present embodiment, if the delivery of the group of data segments "times-out", a request for re-transmission of the group is sent to the transmission server, and a re-transmission counter is incremented, step 430. In the present embodiment, the counter is maintained to enable a maximum allowed number of re-transmission requests. The transmission counter is stored and accessed in a memory, step 432.

If the maximum number of allowed re-transmissions has been exceeded, the group of data segments is considered invalid. In the present embodiment, if even one group of data segments is invalid, the original data object cannot be recovered. In the present example, if the maximum has not been reached, step 434, a re-transmission request for the timed-out data is sent to the originating system, step 436. The time-out counter is then reset, step 438.

When the expected group of data segments is received, step 426, the group is parsed into data segments, step 440. The data segments are then authenticated against the expected delivery pattern record by the receiving system, step 448. In the present embodiment, if that process is successful, step 450, the integrity of the data segment is checked, step 452. This step typically includes checking a hash message digest of the data segment contained the digital signature attached to the data segment. If the integrity check is successful, step 454, the data segment is placed into a memory, "re-assembly area", step 456. In this embodiment, the delivery pattern record for the group of data segments is then flagged as delivered, step 458.

If the Object authentication or integrity check does not succeed, the present embodiment rejects the delivered Object, step 460, and a re-transmission request is generated in step 436, described above, if appropriate.

If the method determines that the delivery process is no longer valid, step 434, for example, the maximum number of re-transmission attempts is exceeded, a transmission failure is reported to the originating system. In the present embodiment, the originating server, or transmission systems, subsequently determines whether or not to re-try transmission of the data. Any data received up to that point is deleted, step 464, and then a delivery failure is written to an application log file, step 466.

Fig. 5 illustrates an embodiment of the present invention where the data segments are re-assembled. Initially, data segments are placed in the storage processing area, step 510, by a previous process of the method, either the Object segmenting process or the discrete data object reception process. Next, the data segments are validated, step 512. In the present embodiment the data integrity and authenticity are checked by analyzing the attached digital signature.

Upon successful validation, the method retrieves storage patterns for this data sequence, step 514. As described above, the storage patterns include specifications for storing the data segments. Initially it is determined whether the data segments should be stored in diverse devices or locations, step 516. This is typically specified by the storage patterns. If this is so specified, the method writes the data segments into diverse location and device storage areas for each data segment according to the respective metadata, step 518.

The present embodiment then determines whether the data segments should be stored in diverse system access areas, step 520. This is typically specified by the storage patterns. If this is so specified, the embodiment writes the data segments into diverse system storage areas according to the respective metadata, step 522. The embodiment then sorts the data segments by system access area, making data segments with the same access area contiguous to each other when read, step 523.

In one embodiment, an additional authentication information, step passwords, PIN, smartcard, biometrics, from operators, is provided, step 524. The present embodiment then Perform authentication and access procedures to confirm it's a ability to establish a connection and session with each system access area specified in the storage pattern record, step 525.

The present embodiment then begins a program loop that stores the discrete data objects according to the contents of the metadata associated therewith. The embodiment then retrieves a discrete partial object that has been placed in the storage processing area according to the method, step 526. Next, the storage metadata of that object is then read to
5 determine that access area and target storage location for the object, step 528. If the target access area for the data write is different than the method's current login area, it logs into the new specified access area, step 529.

The present embodiment then writes the current discrete partial data object to the specified location or device, step 530. The integrity of data write is then verified, step
10 532. The embodiment then determines if all of the data objects have been written and verified, step 534. If not, the method retrieves data objects, step 526, until all have been stored as specified in the storage pattern record. When this occurs, the method logs off from its current system access area, step 536, and logs the storage event in an application log, step 538.

15 Figs. 6-8 illustrate flow diagrams of another embodiment of the present invention. Generally, Figs. 6-8 describe embodiments where, instead of transmission of segmented data across diverse transmission media, transmission paths, and the like, the segmented data is stored onto diverse media, at diverse media locations, and the like. For example, the storage media may be at locations within a local disk drive, within a controlled
20 access storage, the storage media may include tape drives, cd-roms, printed media, and the like. Further the storage may occur at remote sites, for example onto remote servers on a local area network, across a wide-area network, such as the Internet, and the like.

Fig. 6 shows the procedures executed by the method on the retrieval system to reliably retrieve discrete partial data objects that were stored according to the method as
25 described in Fig. 5. In this embodiment, the retrieval process receives a retrieval request for a set of discrete partial data objects, step 610. The retrieval process of the method then validates the request, step 612, passed to it, both for authenticity and for feasibility of the retrieval of each object. Upon successful validation, the method retrieves storage metadata for this object set, step 614, containing specifications as to the location, device, and access
30 area in which the discrete partial data objects are stored. The method first determines whether the metadata specifies that the partial data objects are stored in diverse devices or locations, step 616. If this is so specified, the method retrieves location and device storage

metadata for each Object, step 618. The method then determines whether the metadata specifies that the discrete partial data objects are stored in diverse system access areas, step 620. If this is so specified, the method retrieves system access storage metadata for each Object, step 622. The method then sorts the metadata by system access area, making
 5 metadata records with the same access area contiguous to each other when read, step 624. The method then optionally obtains further authentication information, step passwords, PIN, smartcard, biometrics, from operators or otherwise, step 626, if such an action conforms to the security model of the entity deploying the method. The method then Perform authentication and access procedures to confirm it's a ability to establish a connection and
 10 session with each system access area specified in the storage metadata record, step 628.

The method then begins a program loop that retrieves discrete partial data objects according to the contents of the storage metadata. The method logs onto the system access area specified in the first Object's metadata, step 630. If the target access area for the object retrieval is different than the method's current login area, it logs into the new specified
 15 access area. The method then accesses the specified location or device, step 632. The method then copies the discrete partial data object from that location or device to a retrieved object processing area, step 634, The method then verifies the integrity of data object read, step 636. The method then determines if all of the data objects have been retrieved and verified , step 638. If not, the method retrieves data objects, step 630, until all have been
 20 copied to the retrieved object processing area. When this occurs, the method logs off from its current system access area, step 640, places the retrieved objects into the "re-assembly" system processing area, step 642, and logs the retrieval event in an application log, step 644.

Fig. 7 summarizes the re-assembly process according to one embodiment of the present invention. In step 710, Identify Objects in re-assembly area; in step 712, Transmit
 25 Discrete Partial Data, in step 714, Store objects, in step 716, Authenticate Discrete Partial Objects, in step 718, Determine Object Pattern Identifier, in step 720, Verify Object Integrity and Completeness, in step 722, Retrieve "re-assembly" patterns for this object sequence, perform subsequent actions according to "re-assembly" pattern, in step 724, Parse segments from Discrete Object, in step 726, Discard "false" segments, in step 728, Decrypt re-
 30 encrypted segments, in step 730, Re-order and Combine segments into original data object according to "re-assembly" pattern, and in step 732, Place in processing area for decryption

and general processing. Many of the above techniques were previously described in conjunction with the re-assembly of the first embodiment described.

Figs. 9 and 10 illustrate embodiments of the present invention. In particular, Fig. 9 illustrates that communications networks may include computer backbone networks, 928-932, and may include wireless or land line switching networks 960, 962, 968. As can be envisioned in light of the description of embodiments above, data transmitted from a data origination system 910 may be segmented and the segments may be transmitted to multiple transmission networks. Similarly, the receiving system 950 may receive transmissions from multiple transmission networks, validate the data, and re-assemble the data.

Fig. 10. illustrates that storage media may include media maintained at a variety of physical locations, for example, via the internet, 1040, on a local tangible media, 1052-1-56, on a controlled access storage 1046, and the like. As can be envisioned in light of the description of embodiments above, data transmitted from a data storage system 1010 may be segmented and the segments may be stored to multiple storage media. Similarly, when attempting to re-assemble the data, the data storage system 1010 may receive data from a variety of different storage media at different storage locations. Once validated, the data can then be re-assembled.

20

Conclusion

In the foregoing specification, the invention has been described with reference to specific exemplary embodiments thereof. Many changes or modifications are readily envisioned.

25

Another example, the above described methods may be combined with additional methods and apparatus to provide additional levels of security. For example, biometric measurements may be made for both the senders and receivers to verify the person sending the data or the person retrieving the data are the authorized parties. Examples of biometric measurement embodiments, even where measurements of possible diverse biometric data are combined in a secure manner are described below. The encoding scheme of such measurements can vary, according to the description below. Further, the encoding

30

scheme for the groups of data segments may be according to predefined permutations, as will be described below. In some embodiments of the present invention, dynamic data delimiter methods may be used where validation values are used based upon antecedent data to determine digest values for subsequent data. Further description of embodiments are also
5 described below.

Method and Process for Encoding Biometric or Robometric Measurements

This Aspect of the invention describes a method and process for encoding measurements generated by a biometric or robometric (attributes unique to a specific instance of a machine, electronic circuit or computing device or algorithm) measurement device, and
10 further, transforming that encoding into a value that can be used in common code uses, such as identification or authentication.

An advantage of such a process is that the resultant encoding can be used and distributed as an authentication code such as an encryption key, password, hash number, or PIN number without the need to memorize, record, or expose the actual biometric or
15 robometric measurement itself.

An advantage of such a process is that the authentication code so generated can be re-generated by the process if the authorized generator of the code forgets or loses the authentication code.

Another advantage is that the authentication code can be cross-checked against
20 a biometric or robometric measurement of the presenting entity, either taken at the time of presentation or by comparison to a referential record, to determine if the presenter of the code is the entity authorized to use the code.

Another advantage of this process is that many different codes can be generated by utilizing different computational methods that allow biometric or robometric
25 measurements to be manipulated in different ways.

Another advantage of this process is that it reduces the probability of the same code representing different entities since the metric input generating the code is highly unlikely to be the same between two entities.

Another advantage of this process is that it allows unique biometric or
30 robometric measurements to be used in authentication without exposing the measurements themselves to the authenticating process or to transmission over a public network, since the

algorithm which generated the corresponding code, key, or PIN number can be kept secret, thereby concealing the measurement that was input into it.

Another advantage of this process is that it removes the requirement of authenticating process to maintain a database of authorized entity authentication codes since the entity can be reliably authenticated by receiving both an authentication code and one or more metric measurements and simply calculating a match between them. The entered code and measurement can then be logged by the access process to create an access history if needed, which can then be compared to a database at a later time.

Another advantage of the device is that it reduces the probability of defrauding or "spoofing" a biometric or robometric input device, or an authenticating code input device, since the presenter of fraudulent measurements or codes must be able to simultaneously present the corresponding code or measurement.

The Method and Process for Generating Authentication Codes from Biometric or Robometric Measurements can receive measurement input from standard biometric measurement devices such as fingerprint readers, eye scanners, voice print recognition systems, face or hand geometry analyzers, or other such devices that measure an attribute of the human body or actions thereof. It can also receive input from robometric measurement devices or processes such as ROM-embedded identifier retrieval systems, emitted frequency analyzers, activity log analyzers, or other such devices or processes that reveal attributes of a specific instance of a machine, circuit, process, or algorithm.

The Process described herein can then take this input biometric or robometric measurement and manipulate it in such as way as to produce a code, encryption key, hash, PIN number, or other such authenticating identifier which can be associated with the metric measurement generating entity.

The algorithm by which the input metric measurement data is manipulated can be varied to produce different types of authenticating codes or different codes within the same type. This algorithm can use a hashing algorithm, a sum difference calculation on the metric measurement input stream, a CRC calculation algorithm, or any such data manipulation algorithms to output a code confirming to the requirements of the authenticating system.

The authenticating system could be a public-private key pair for a session key or for a digital certificate such as those used in the Public Key Infrastructure system, a logon

password such as those commonly used on computer networks, or a PIN number such as those commonly used in banking or other automated transaction verification systems.

If the authentication system analyzing the code input, metric measurement input, or combination thereof detects a mismatch or fraudulent use of the code, measurement, or combination thereof, it can prevent further access or use of the system, process, or device requiring appropriate authentication. It can then also log such use and report it to a process for correction, retry, cancellation, or notification of such use of the code, measurement, or combination thereof.

The Process can also be used to record and prove legitimate use of computing or other devices at a specific time, such as employee time cards, financial transactions, remote voting, or sender/receiver verification in electronic communication.

The drawing in Fig. 11 shows a process flow for generating codes, encryption keys, or PIN numbers in the Method and Process for Generating Authentication Codes from Biometric or Robometric Measurements. A biometric or robometric measurement device or process initiates an action to produce a data stream representing such measurement. It then passes this data stream to an algorithm executing on a computing device that transforms the measurement into a code, key, or number in the format required by the target authentication system. This code, key, or number is then passed to the measured entity for later or subsequent use with the authentication system. Subsequent use can be instantaneous or deferred to a later time.

The drawing in Fig. 12 shows a process flow for cross-checking presented codes, encryption keys, or PIN numbers against Biometric or Robometric Measurements. The presenting entity (human, machine, circuit, or process) presents the code, key, or PIN number derived from algorithmic manipulation of a bio/robometric measurement to an authenticating process. A biometric or robometric measurement device or process simultaneously or subsequently initiates an action to produce a data stream from a measurement of the presenting entity. It then passes this data stream to an algorithm executing on a computing device that transforms the measurement into a code, key, or number in the format required by the target authentication system. This code, key, or PIN number is then compared to presented code, key, or PIN number to determine if the presenting entity is the authorized presenter. If a match occurs, the authenticating process

allows access to the restricted process. If a match does not occur, the authenticating process executes a mismatch procedure, possibly not allowing access to the restricted process.

Device Comprising Two or More Diverse Biometric or Robometric Measurement Devices

5 Further disclosed in this Aspect of the invention is a device comprising two or more biometric or robometric measurement devices which simultaneously or sequentially receive diverse inputs from a human, machine, circuit, or process. These measurements can be used to authenticate the identity or specific instance of the subject being measured.

10 An advantage of such a process is that the subject can be measured in a manner that is more reliable than that which is achievable from the measurement of a single attribute of the subject.

Another advantage of such a process is that the subject can be measured in more than one manner with less intrusion on the subject than measuring the subject with two or more separate devices. The Device herein disclosed can be designed so that it
15 simultaneously measures diverse aspects of the subject from a single action or state associated with the subject, instead of requiring multiple actions or states on the part of the subject being measured. Multiple measurements of the subject are more likely to be taken if the process of measuring multiple attributes is as easy and non-intrusive as measuring only one attribute of the subject.

20 Another advantage is that the device can be manufactured for a lower cost and operated with lower analysis system requirements than that of two or more separate systems, each requiring its own power supply, cabling, case, probe, or processor time.

Another advantage of this process is that can allow different combinations of measurements to be taken which allows the Device to provide measurements to a variety of
25 authentication and analysis systems with varying measurement requirements.

Another advantage of the Device is that it is more difficult for the subject to simulate the identity of another subject entity since the fraudulent subject would be required to simulate more than one subject attribute.

Another advantage of this device is that it reduces the probability of the same
30 measurement occurring in two different subjects since it is much less likely that they would provide the same measurement from two or more diverse authenticating measurements.

The Device Comprising Two or More Diverse Biometric or Robometric Measurement Devices can comprise two or more measurement devices commonly used in biometric measurement methods such as fingerprint readers, eye scanners, voice print recognition systems, face or hand geometry analyzers, signing analyzers, or other such devices that measure an attribute of the human body or actions thereof. It can combine two or more of such devices into a single device designed so as to increase the ease of use of both devices in a manner which could not be achieved if the biometric measurement methods were contained in separate devices.

It can also combine two or more robometric measurement devices or processes such as ROM-embedded identifier retrieval systems, emitted frequency analyzers, activity log analyzers, or other such devices or processes that reveal attributes of a specific instance of a machine, circuit, process, or algorithm.

The Device described herein can perform these diverse biometric or robometric measurements simultaneously or in rapid sequence so as to only require one intrusion, interruption, state or action on the part of the subject being measured. This increases the probability that multiple measurements will be taken and allows the measured subject to operate more efficiently.

The measurements taken by the Device can be varied to produce different types of identifying signals depending on which types of measurement devices are combined into the Device. This would allow the Device to be used as a measurement Device for a wide variety of authenticating systems requiring different types of measurement inputs.

Fig. 13 discloses one embodiment of the device used for biometric authentication which is comprised of devices for measuring multiple fingerprint patterns, palm print patterns, iris patterns, and voice prints simultaneously or in rapid sequence. The subject places both hands on the Device on fingerprint and palmpoint pattern sensing areas 10 and 20. In this embodiment, these areas are comprised of capacitance sensing semiconductors which provide electronic signals representing the hand print pattern to a pattern analysis device. These and pattern sensing areas could also be comprised of an optical imaging system, which delivers optical data to a pattern analysis system. Upon sensing the presence of hands, the Device begins to gather pattern signals for analysis. The subject then raises the Device so that lenses 30 and 40 are level with the eyes. This places the lenses in an appropriate position to gather images of the left and right irises of the subject's eyes. The

subject then speaks predefined or random phonetics towards microphone 50. Upon sensing input to the microphone, the Device transmits to a pattern analysis device the patterns from the fingerprint and palmprint pattern gathering areas, patterns from the iris image areas, and an electronic representation of the signal generated by the microphone receiving phonetic input from the subject for voice print analysis.

Method for Combining Two or More Diverse Biometric or Robometric Measurements into a Single Value

Further disclosed in this Aspect of the invention is a method for combining two or more diverse biometric or robometric measurements into a single value, signal, code or representation of the combined measurements.

An advantage of this process is that allows more efficient processing and comparison of diverse biometric measurements since the processing operations on a single value is faster and less complex to program.

Another advantage of this process is that it is more efficient to transmit combined diverse biometric measurements in a single value due to lower bandwidth requirements.

Another advantage is that the combined diverse biometric measurement value can be used to generate encryption keys, codes, passwords, and PIN numbers that are more difficult to forge or duplicate due to the increased complexity of recreating the measurements that generate the combined value.

Another advantage is that the combined biometric measurement's authentication rejection rate is more reliable than that generated from a single biometric measurement due to the increased certainty inherent in requiring multiple measurement matching.

Another advantage is that the combined biometric measurements can be encoded in the Value so that the biometric measurements themselves cannot be reversed out or discerned from the Value, thereby protecting the privacy of the biometric measurement.

Conversely, another advantage of the process is that the combined biometric measurements can be encoded in the Value so that the biometric measurements themselves can be reversed out or discerned from the Value, thereby allowing storage of multiple biometric measurements more efficiently as a single record.

Another advantage is that the Value could be a common input to the analysis process of a wide variety of single and multiple measurement devices, since the measurement(s) they require to match against can be extracted from the combined Value.

Another advantage to the process is that its resultant values can create a
5 valuable contribution to research investigating the relationship between biometric attributes of the human body since a database of these accumulated measurements would contain uniform representation of diverse human biometric attributes.

Another advantage of this process is that it reduces the probability of the same measurement value occurring between two different subjects since it is much less likely that
10 they would provide the same value when diverse multiple measurements are combined.

Another advantage of this process is that it allows diverse biometric measurement to be gathered at different times or in different places and stored in such a way as to organize them in one record for easier reference.

The Process can comprise various sub-processes that receive as input the
15 signals generated by two or more diverse biometric measurement devices, manipulate, combine and encode those signals by means of a mathematical formula, relationship calculation, determination of relative characteristics in time or space, or other such means, and output a value compliant with requirements for size, resolution, reversibility, or other requirements.

20 Biometric measurement devices providing the signals into the Process can include devices commonly used in biometric measurement methods such as fingerprint readers, eye scanners, voice print recognition systems, face or hand geometry analyzers, signing analyzers, or other such devices that measure an attribute of the human body or actions thereof. The measurements generated by these devices can occur simultaneously or
25 sequentially and in one or more geographic locations.

In one possible embodiment, the process receives the signals generated by the biometric measurement devices and manipulates them according to an algorithm to produce the desired output. For example, the process may receive input from multiple biometric devices that measure voice print patterns through time, written signature pen pressure and
30 spatial coordinates through time, fingerprint patterns, and iris patterns. The process would create a result record that included information about the sources of the input measurements.

The process could take these diverse measurements and manipulate them in different ways to satisfy a variety of result value requirements. For example, if the result combined measurement value needed to be reversible to allow specific measurements to be extracted, the Process could interleave the measurements in a predefined structure which
5 would be known to a process designed to extract a measurement. This could be sequentially and consecutively placing two bytes from each of the four input measurement data streams in the example embodiment.

If the result value needed to be small in size, perhaps to fit in limited micro-processor memory or to be transmitted on a low bandwidth medium, the Process could
10 remove information from each measurement according to a predefined pattern prior to combining the measurements. This could be removing every fourth byte from the data stream of each measurement, or some such lossy measurement manipulation. The structure of information removal would be known the target analysis system so that it could manipulate biometric measurements it receives to produce similar comparison values. By combining
15 diverse measurements into a Value in which information is lost, higher reliability is created in the subject authentication process, or other applications of using the result Value, than can be achieved with lossy manipulation of the biometric measurement from a single source.

If so required, the example embodiment could produce a non-reversible result combined Value whereby the source biometric measurements could not be extracted from the
20 result combined Value, perhaps in order to protect the privacy of measured source subject, or perhaps to foil misuse of a biometric measurement extracted from the Value. The example embodiment could accomplish this by XORing the four data words from identical positions in the four input data streams, or by adding the binary value of a user PIN number to consecutive interleaved bytes in the combined measurement Value. This latter sub-process
25 would allow the source biometric measurements to be unlocked for extraction by a process that knows the encoding PIN number. This process could similarly use encryption or hashing to produce result combined Values which are private or non-reversible, or both.

Similarly, the example embodiment of the process could calculate a result process based upon the mathematical relationship of the source measurements. For example,
30 the Process could take signature pressure and coordinate measurements values, add them together, and subtract the result from voice print values which occur at the same point in time. It could then take fingerprint patterns and add them to iris scan patterns which occur

within the same relative spatial area of their respective scan fields. The resulting time and spatial calculation data streams could then be XORed to further obfuscate the source measurements. The authenticating process wanting to verify the subject identity could manipulate biometric measurement inputs in an identical way to create a data stream which
5 could be compared to the result combined Value data stream.

Dynamic Data Delimiter Method

Further disclosed in this Aspect of the invention is a Method for delimiting data for recognition and processing by a data analysis system. The Method inserts a demarcation value into a data stream followed by a subsequent value that is dynamically
10 calculated by a digesting algorithm from the data that follows it. The analyzing process recognizes the demarcation value, then calculates a validation value based on antecedent data. It then compares the calculated digest value to the value in the data delimiter to validate the function of the delimiter and the integrity of the antecedent data.

One advantage of the Method is that it provides a more reliable and less error
15 prone indicator of the beginning or end of a data stream or data field.

Another advantage of the Method is that it provides a check on the validity of the data within the data stream since the digest calculation of that data must match the digest value contained in the delimiter.

Another advantage of the Method is that it operates efficiently on inexpensive
20 microcomputers.

Another advantage of the Method is that the demarcation value allows it to be used to signify a diversity of types of data streams.

The drawing in Fig. 14 shows the features of the Dynamic Data Delimiter Method. The Method is comprised of steps of capturing the data to be delimited, calculating
25 beginning and ending digest values from a portion or all of a data stream, inserting the beginning demarcation value at the beginning of the data stream, subsequently inserting the calculated digest value after the demarcation value at the beginning of the data stream, inserting the ending demarcation value at the end of the data stream, and then inserting the ending digest value after the ending demarcation value. The data object now consists of the
30 original data stream plus the inserted beginning and ending demarcation values and digest values.

The analyzing processing system later reads a data stream with the delimited data object embedded into it. The analyzing system finds the beginning demarcation value, retains the digest value, and then proceeds to calculate the digest value of subsequent data stream values as specified by the parameters of the original digest algorithm that calculated the beginning delimiter digest values. If the digest value calculated by the data analysis system matches the value embedded in the data delimiter, the analysis system assumes that the delimiter is valid and proceeds to process the data stream as the type described by the delimiter. When the analysis system finds the ending demarcation value in the data stream, it calculates a digest value of precedent data stream values as specified by the parameters of the original digest algorithm that calculated the ending delimiter digest values. If the ending digest value calculated by the data analysis system matches the value embedded in the data delimiter, the analysis system assumes that the ending delimiter is valid and assumes that the data stream of the type described by the delimiter is ended. The ending delimiter type must be the complement of the beginning delimiter type.

15 Method for Encoding Data by Permutation Ordination

Further disclosed in this Aspect of the invention is a Method for Encoding data by representing the data by the value of its order in a permutation table rather than the data value itself. Since storage of successive data values in this manner could require less storage than storing the actual values they represent, and since decoding the values is difficult without knowledge of the representation of the permutation tables, the Method allows advantages in the saving of storage requirements and in the privacy of stored or transmitted data. This process also compresses data by symbolizing it as a permutation ordination of bit groupings so as to require fewer digits to express the same value in the base two number system. This process also increases the possibility of effective compression by altering the patterns of the data stream (data alteration) in a predefined and systematic way.

In the encoding by Permutation Ordination Method, bit combinations of varying width are tested for series of unique or pre-defined combinations of groupings of 1's and 0's. If an appropriate series of groupings is found, it stores the permutation reference for that combination of groupings instead of the groups of actual bits. This can result in savings of 1 to 4 bits per groupings of 16 to 32 bits, depending on the permutation basis (i.e., 6 unique/ pre-defined groups of 5 bits, 8 unique/pre-defined groups of 6 bits, etc.). Enough

consecutive unique bit groupings must be found to allow a bit savings large enough to compensate for the overhead of storing the permutation indicators.

In a simple example, the 3 bit wide bit groupings of (000) (001) (010) could be represented by the number (00000001) since they are the first possibility of unique permutation bit groupings in that bit width category. Storing the number (00000001) instead
5 of the source data would provide one saved bit in storage.

The unique permutation ordinations are translated back into their bit groupings by the formula:

$$P/n/n-1/.../n-k = \text{number of rows of each element in column } n + \text{offset is equal}$$

10 to the value -count of lesser previous items.

Pre-defined tables of bit combination groupings may be used to supplement permutation tables and increase the number of bit groupings that can be represented by a binary number of fewer digits.

The Permutation Ordination Method compresses data by symbolizing it as a permutation ordination of bit groupings so as to require fewer digits to express the same
15 value in the base two number system.

The Method allows data in the nature of unique or non-repetitive (random) bit groupings to achieve good lossless compression. This creates the possibility for recursive data compression, producing a result file of a compression process that can be compressed
20 even further by the same process.

Bit combinations of varying width are tested for series of unique or pre-defined combinations of groupings of 1's and 0's. If an appropriate series of groupings is found, it stores the permutation ordination reference for that combination of groupings instead of the groups of actual bits.

For example, there are 1680 possible combinations of four unique sets of three
25 bits per set. The position within the 1680 unique permutations can be recorded in 11 bits (up to 2048) even though the source data is 12 bits wide. This results in a one bit saving. Enough consecutive unique bit groupings must be found to allow a bit savings large enough to compensate for the overhead of storing the permutation indicators. The process can switch
30 among pre-defined permutation tables to allow for increased probability of finding a permutation sequence which provides a savings of stored bits.

In this example, the 368 remaining bit combinations (1680-2048) which can be represented in the 11 bit compressed data can be pre-defined as compressible combinations to allow greater possibility of enough consecutive compressible bit groupings to compensate for process overhead.

5 The unique permutations ordinations are translated back into their source bit groupings by the formula: $P/n/n-1/.../n-k = \text{number of rows of each element in column } n + \text{offset value} - \text{count of lesser previous items}$.

10 In the permutation ordination method of data compression, tables of pre-defined bit combination groupings, not just unique groupings, may be used to supplement permutation tables and increase the number of bit groupings that can be represented by a binary number of fewer digits. One could even use this method by dynamically creating arbitrary or pre-defined tables of bit groupings based on the bit groupings found in the source data and then storing the ordinations of those bit groupings found in those tables.

15 The block diagrams of the architecture and flow charts are grouped for ease of understanding. However it should be understood that combinations of blocks, additions of new blocks, re-arrangement of blocks, and the like are contemplated in alternative embodiments of the present invention.

20 The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense. It will, however, be evident that various modifications and changes may be made thereunto without departing from the broader spirit and scope of the invention as set forth in the claims.

25 While the above is a full description of the specific embodiments, various modifications, alternative constructions, and equivalents may be used. Therefore, the above description and illustrations should not be taken as limiting the scope of the present invention which is defined by the appended claims.

WHAT IS CLAIMED IS:

- 1 1. A method for transmitting data from a first computer to a second
2 computer comprises:
3 identifying data to be transmitted;
4 segmenting the data into a plurality of data packets, the plurality of data
5 packets including at least a first plurality of data packets and a second plurality of data
6 packets;
7 specifying a first transmission carrying medium for transmission of the first
8 plurality of data packets;
9 specifying a second transmission carrying medium for transmission of the
10 second plurality of data packets;
11 transmitting the first plurality of data packets to the first computer network
12 backbone; and
13 transmitting the second plurality of data packets to the second computer
14 network backbone.
- 1 2. The method of claim 1 further comprising encrypting the first plurality
2 of data packets to form a first plurality of encrypted data packets, and
3 wherein transmitting the first plurality of data packets comprises transmitting
4 the first plurality of encrypted data packets to the first computer network backbone.
- 1 3. The method of claim 1 further comprising:
2 forming a plurality of dummy data packets; and
3 transmitting the plurality of dummy data packets to the first computer network
4 backbone interspersed within the first plurality of data packets.
- 1 4. The method of claim 1 wherein segmenting the data into the plurality
2 of data packets comprises reversibly segmenting the data into at least the first plurality of
3 data packets and the second plurality of data packets.
- 1 5. A method for receiving data from a first computer in a second
2 computer comprises:

3 receiving a first plurality of data packets from a first communications network,
4 the first communications network coupled to the first computer to the second computer;
5 receiving a second plurality of data packets from a second communications
6 network; and
7 processing the first plurality of data packets and the second plurality of data
8 packets to recover transmitted data.

1 6. The method of claim 5 wherein the first communications network
2 comprises a first computer network backbone.

1 7. The method of claim 6 wherein the second communications network
2 comprises a second computer network backbone.

1 8. The method of claim 6 wherein the second communications network
2 comprises a public switched telephone network.

1 9. The method of claim 6 wherein the second communications network
2 comprises a wireless communication system.

1 10. The method of claim 5 wherein processing the first plurality of data
2 packets further comprises decoding the first plurality of data packets.

1 11. The method of claim 5 wherein processing the first plurality of data
2 packets comprises discarding dummy data packets from the first plurality of data packets.

1 12. A computer program product for a computer system having a processor
2 comprises:

3 code configured to direct the processor to retrieve a first plurality of data
4 packets received from a first memory portion;

5 code configured to direct the processor to retrieve a second plurality of data
6 packets received from a second memory portion; and

7 code configured to direct the processor to process the first plurality of data
8 packets and the second plurality of data packets to restore an original object,

9 wherein the codes are resident on a tangible media.

1 13. The computer program product of claim 11 wherein the first memory
2 portion is a local disk drive.

1 14. The computer program product of claim 12 wherein the second
2 memory portion is a remote disk drive

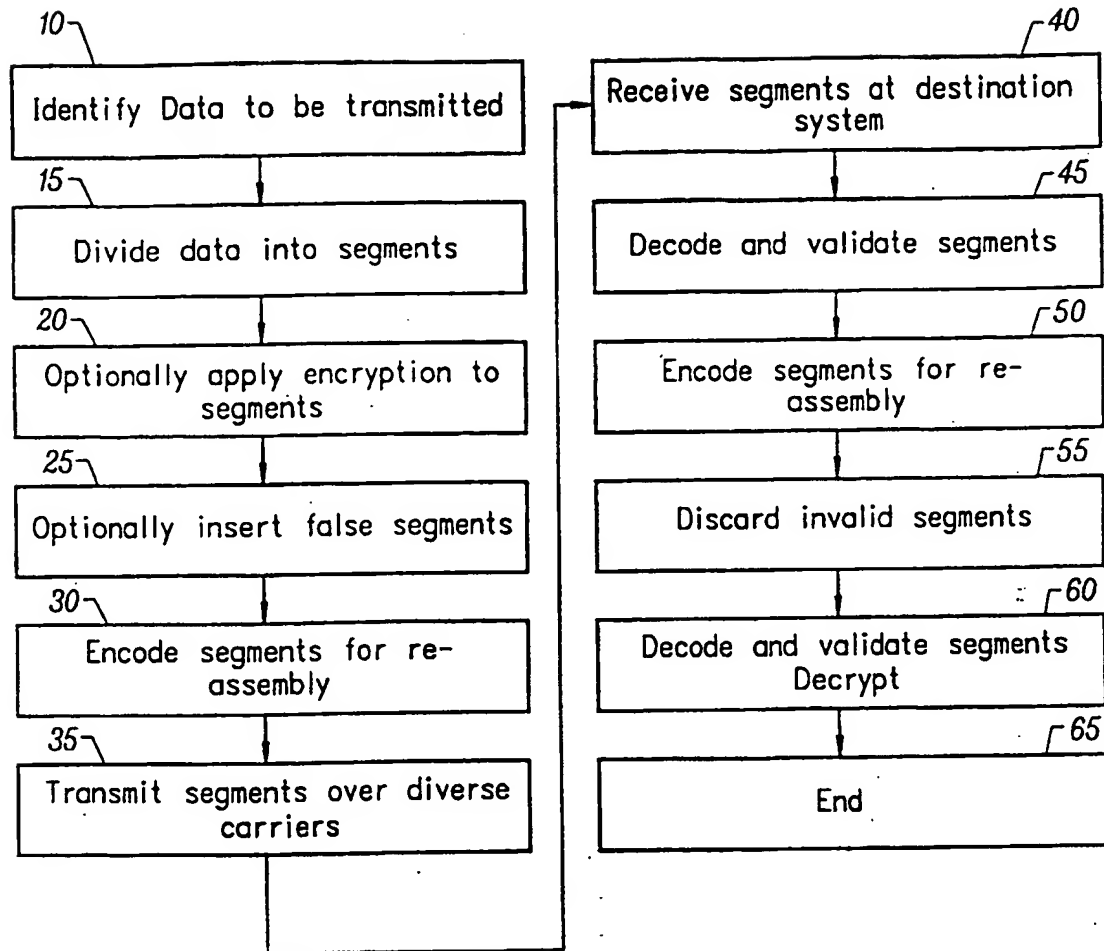
1 15. The computer program product of claim 11 wherein the second
2 memory portion is stored in a separate location from the first memory portion

1 16. The computer program product of claim 11 wherein the code
2 configured to direct the processor to process the first plurality of data packets further
3 comprises code configured to direct the processor to decode the first plurality of data packets.

1 17. The computer program product of claim 11 wherein the code
2 configured to direct the processor to process the first plurality of data packets comprises code
3 that directs the processor to discard dummy data packets from the first plurality of data
4 packets.

1 18. A computer program product storing data from a computer having a
2 processor comprises:
3 code configured to identifying data to be stored;
4 code configured to segment the data into a plurality of data packets, the
5 plurality of data packets including at least a first plurality of data packets and a second
6 plurality of data packets;
7 code configured to specify a first storage medium for storage of the first
8 plurality of data packets; and
9 code configured to specify a second storage medium for storage of the second
10 plurality of data packets.

1/12



System Flowchart

FIG. 1A

2/12

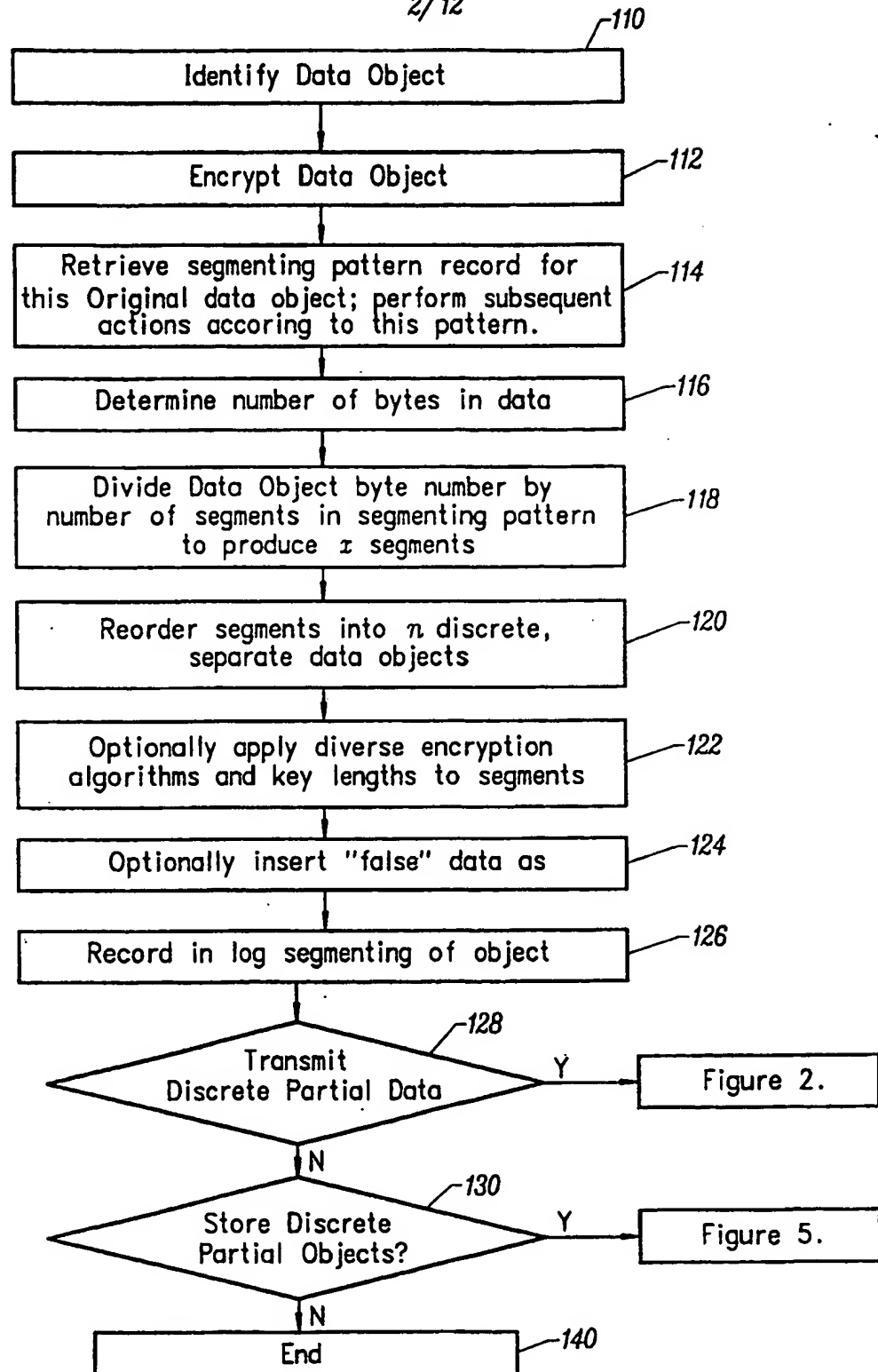


FIG. 1B

3/12

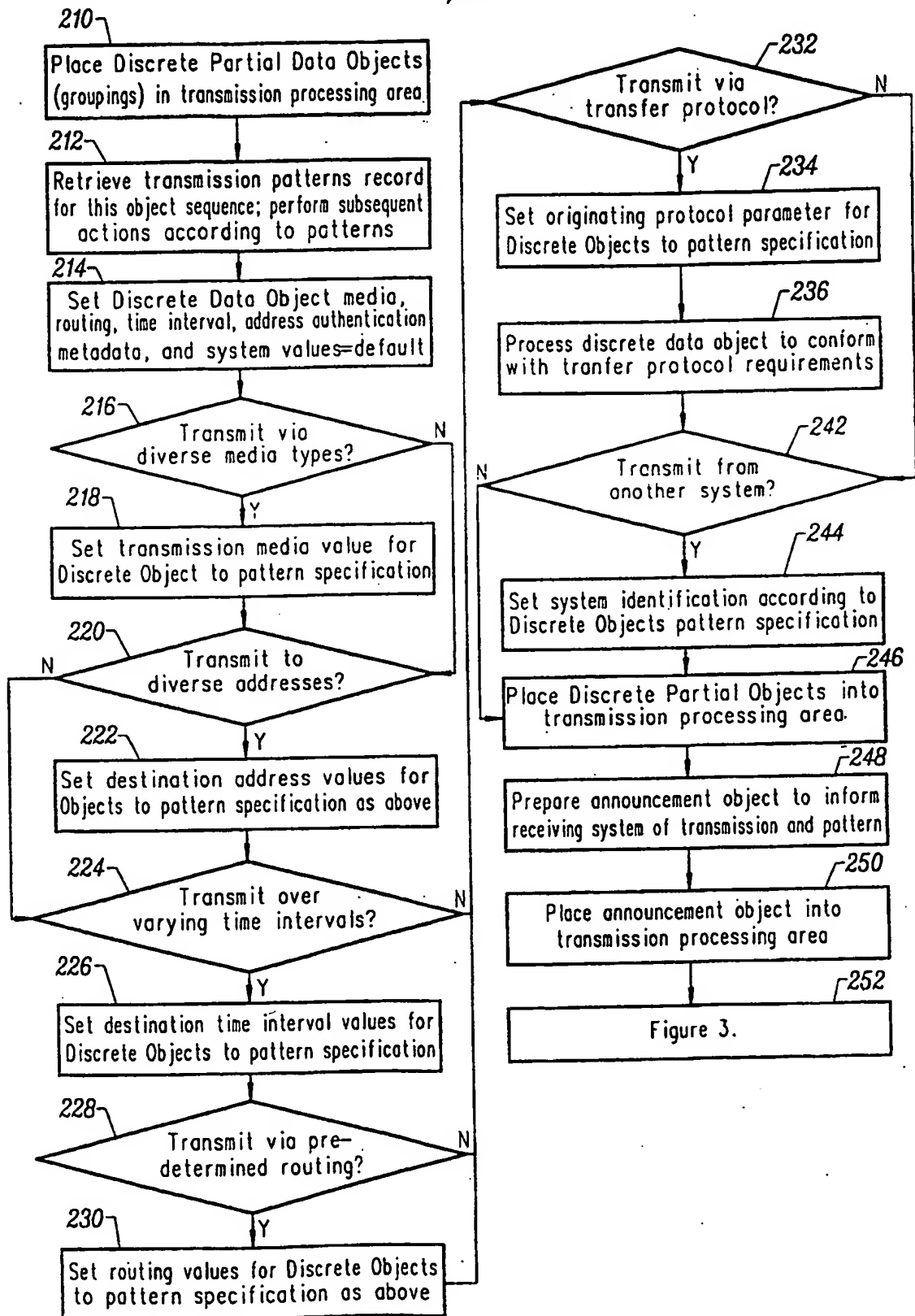


FIG. 2

SUBSTITUTE SHEET (RULE 26)

312-



5/12

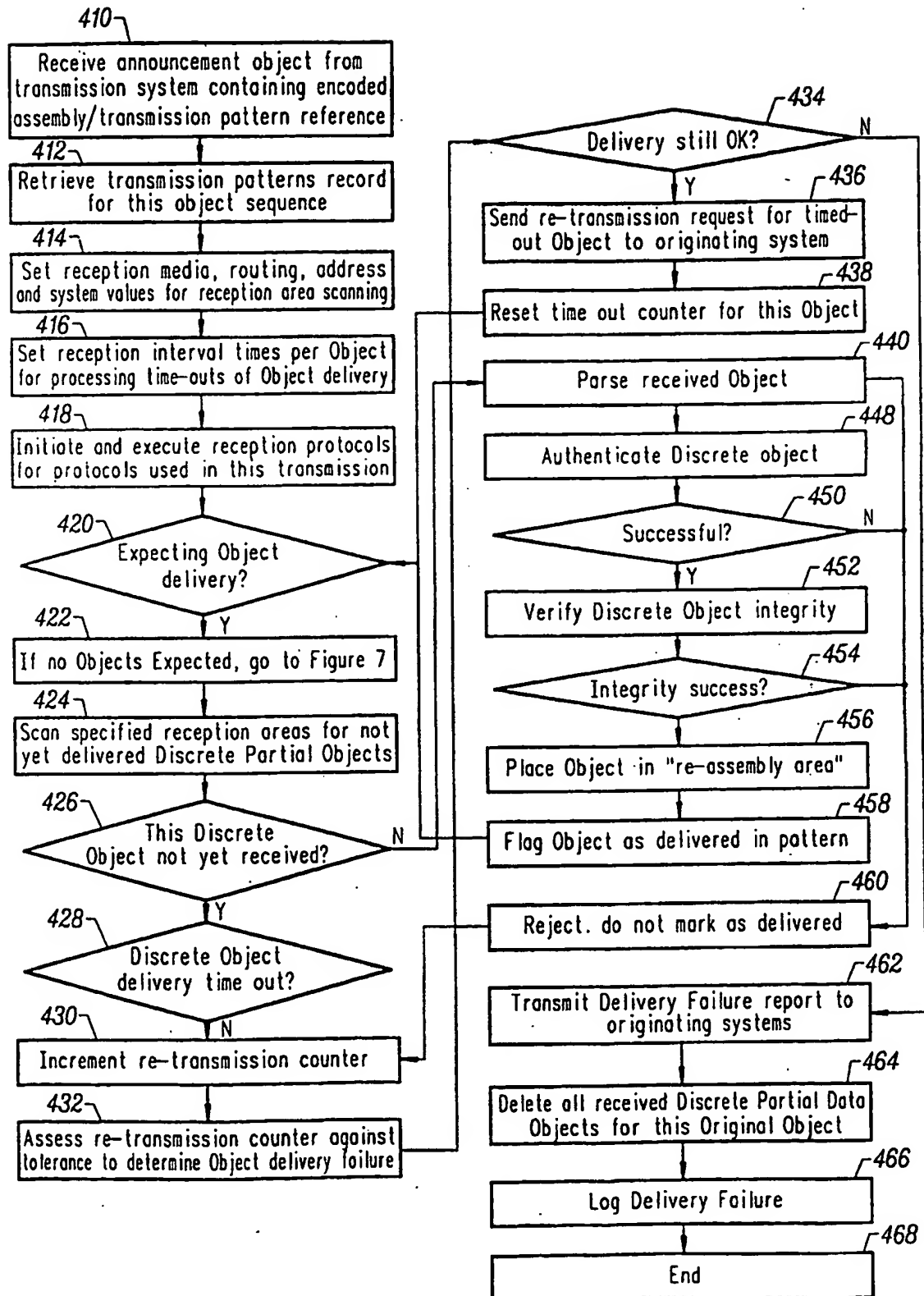


FIG. 4

6/12

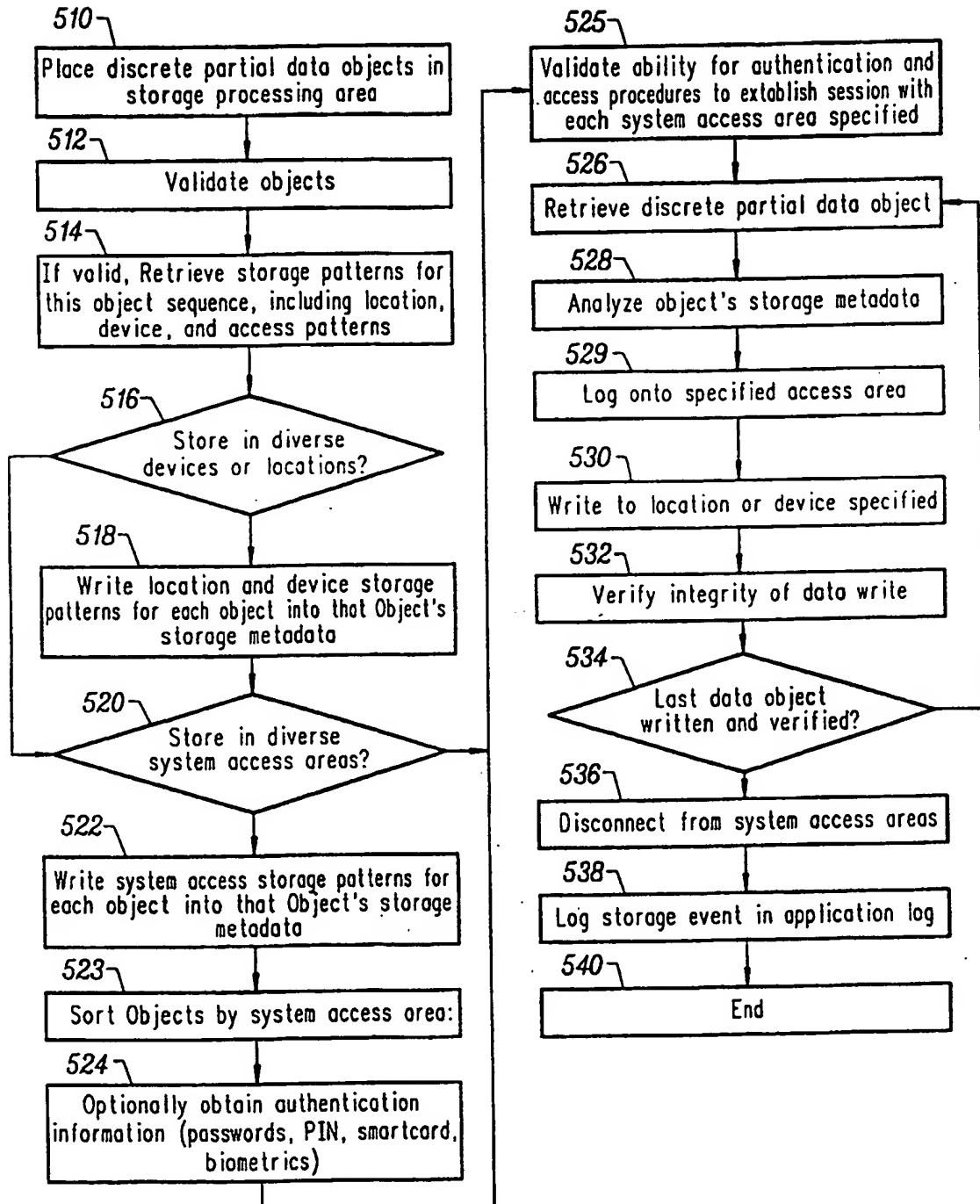


FIG. 5

7/12

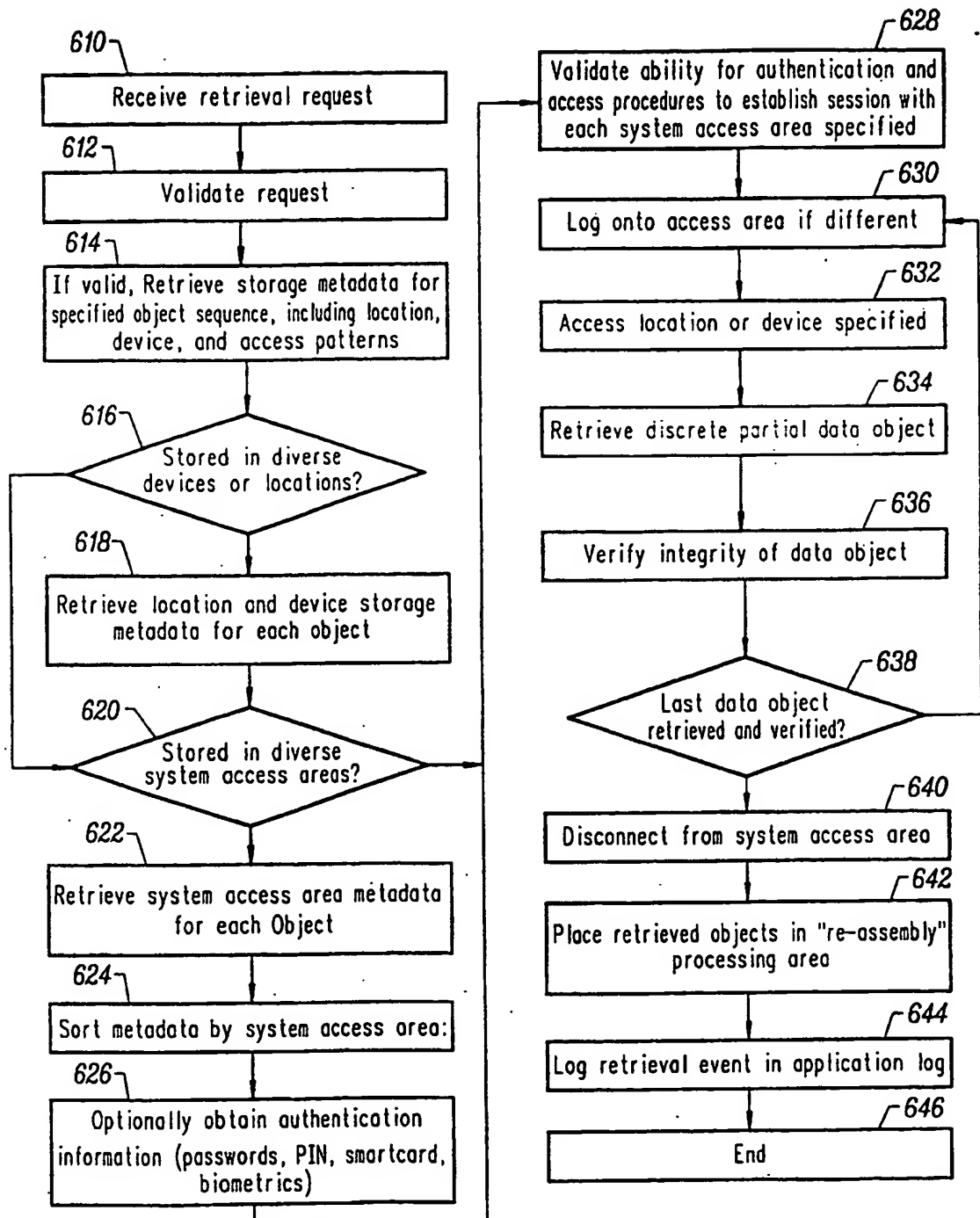


FIG. 6

8/12

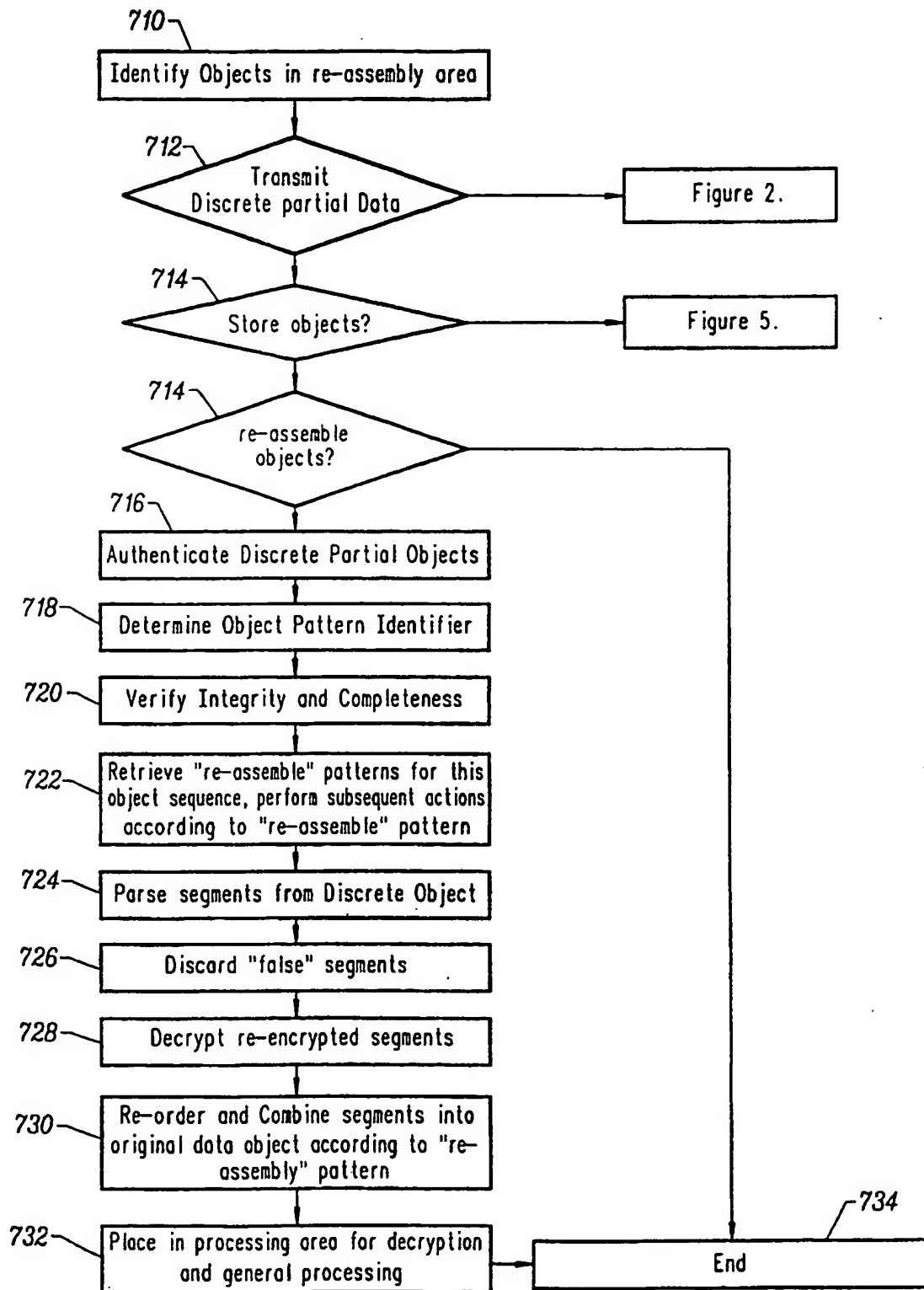
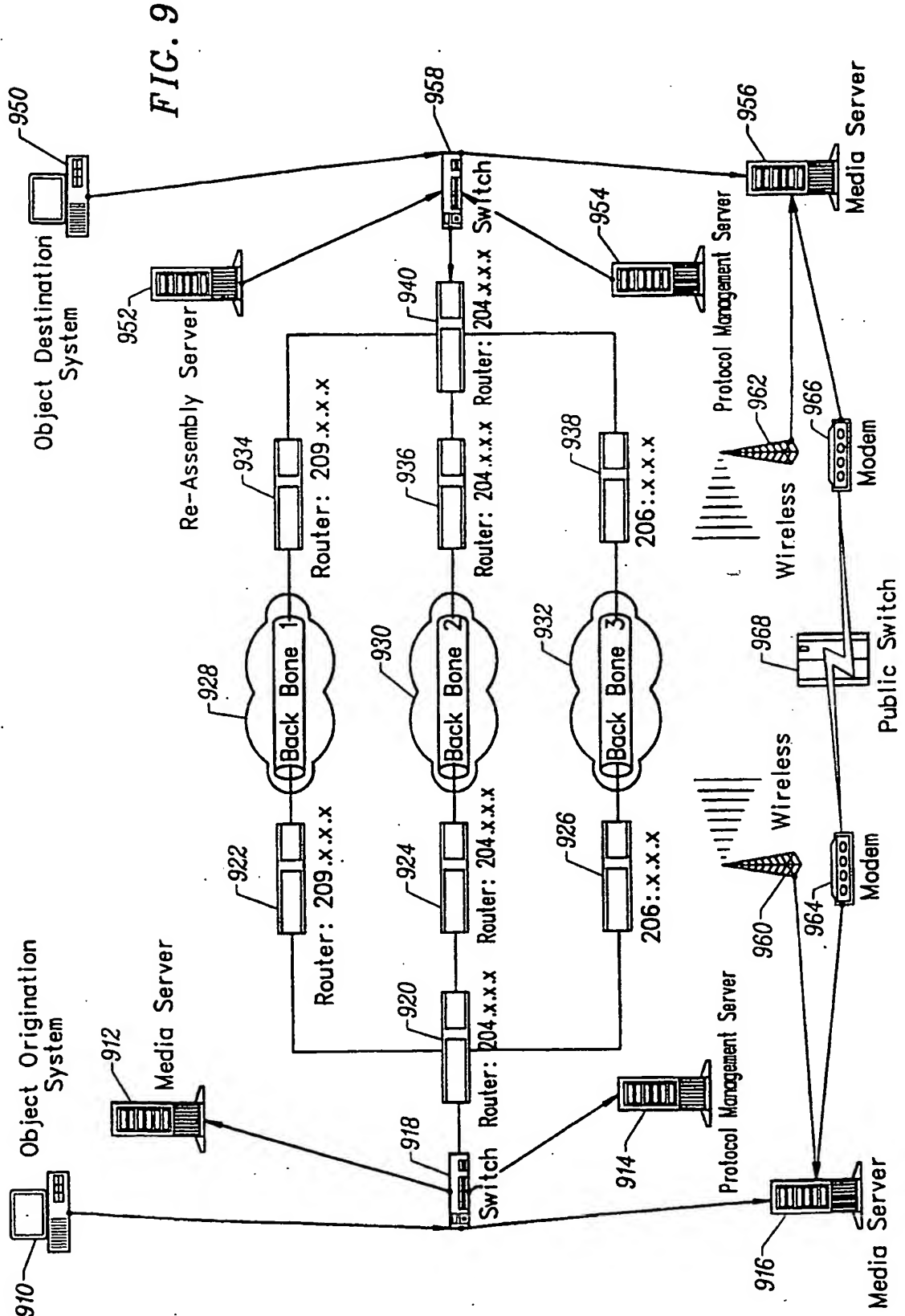


FIG. 7&8

9/12



10/12

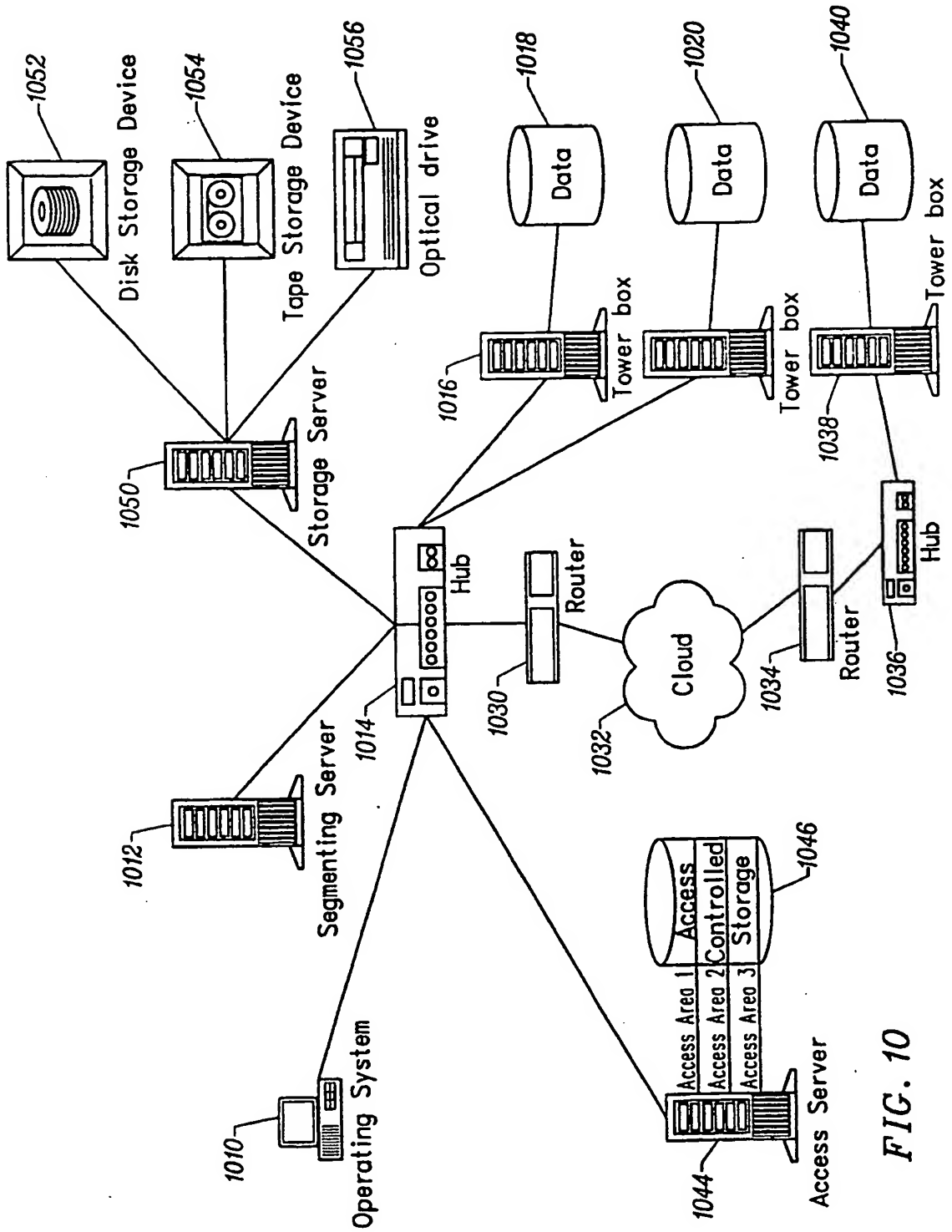


FIG. 10

11/12

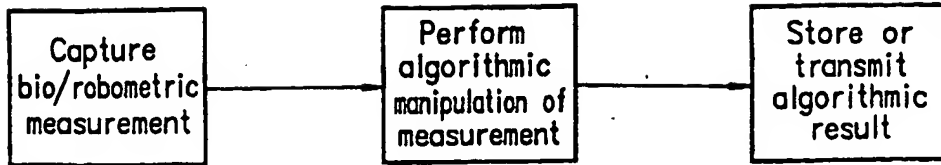


FIG. 11

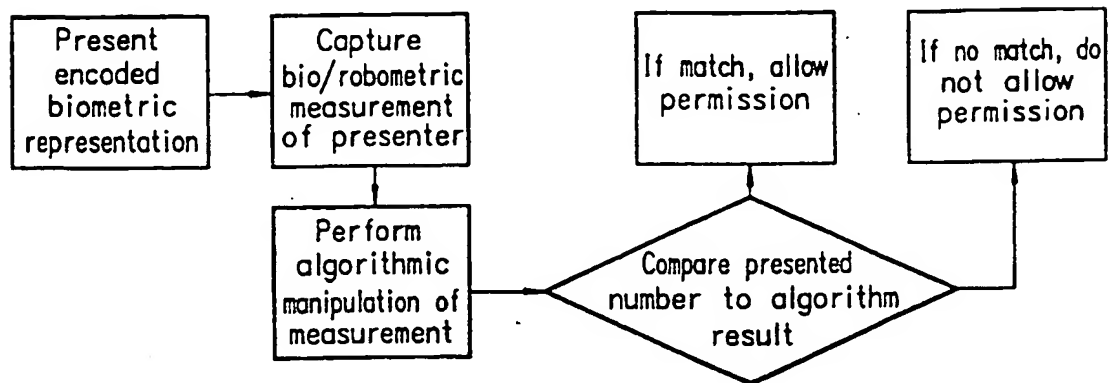


FIG. 12

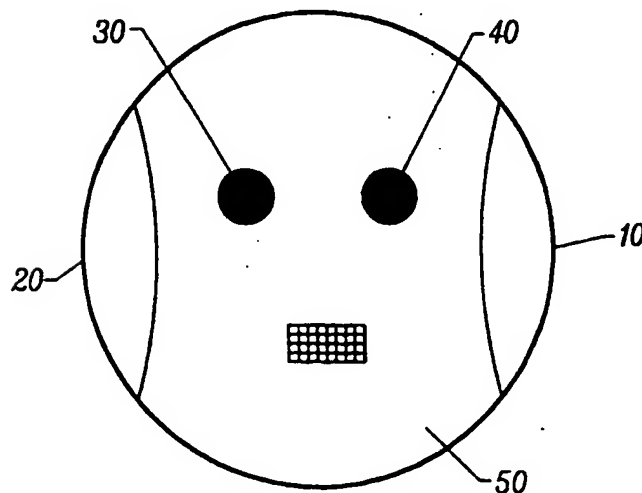


FIG. 13

12/12

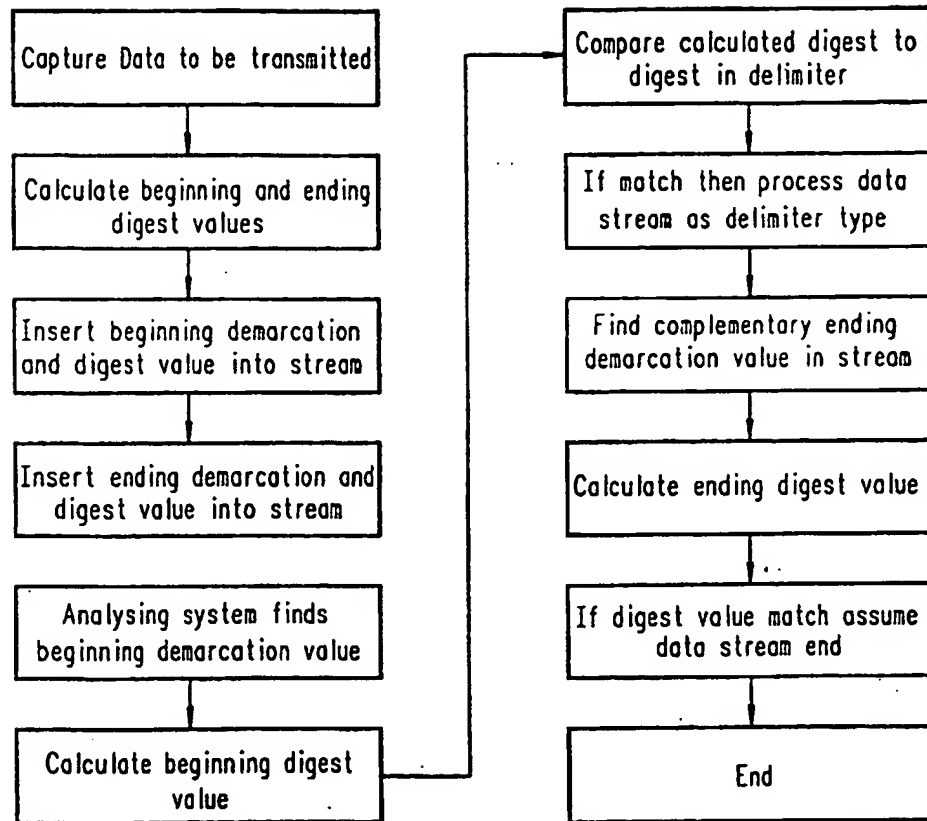


FIG. 14

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/16087

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : HO4L 12/56; HO4J 3/24

US CL : 370/79,474; 380/25,29,23; 455/3.1,5.1,6.1; 714/807

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 370/79,474; 380/25,29,23; 713/200,201; 455/3.1,5.1,6.1; 714/807

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS

search terms: transmit, transmission, send, data packets, segment, encode, encrypt, multiple, plural, network.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,602,853 A (BEN-MICHAEL et al) 11 February 1997, col.1, lines 43-54, col.2, lines 25-30	1-18
Y	US 5,781,549 A (DAI) 14 July 1998, abstract, col.2, lines 34-37, col.13, lines 50-65	1-18
A,E	US 5,953,418 A (BOCK et al.) 14 September 1999, col.21, lines 50-67, col.23, lines 30-44.	1-18
A	US 5,541,919 A (YONG et al.) 30 July 1996, col.3, lines 1-26, col.10, lines 26-37.	1-18

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
A document defining the general state of the art which is not considered to be of particular relevance	*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
B earlier document published on or after the international filing date	*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	*A* document member of the same patent family
O document referring to an oral disclosure, use, exhibition or other means	
P document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

23 SEPTEMBER 1999

Date of mailing of the international search report

18 OCT 1999

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

GAIL HAYES

Telephone No. (703) 305-9711